newera.
TECHNOLOGY

Scott Tunmer

CISSP, PMP®, CSSGB

scott.tunmer@neweratech.com

GRC Practice Lead

Risk Management Fundamentals

Risk Management:

The "Why" Behind Everything We Do in Cybersecurity

November 7, 2025

newera. TECHNOLOGY

Our Goals Are To:

Develop an effective way to Identify, Estimate, and Prioritize Cybersecurity Risk

Promote critical thinking about Risk Management.

Contents

Risk: Why Measure it? What Do We Want to Know?

Compliance and Benchmarking

- Are we meeting all compliance obligations?
- How do our risk practices compare to industry standards?

Risk Assessment

- What risks and threats do we face?
- How likely are they to occur?

Impact Evaluation

- How would risks affect confidentiality, integrity, and availability?
- What are the potential business impacts?

Risk Appetite and Financial Exposure

- Is our Annual Loss Expectancy (ALE) aligned with risk tolerance levels?
- Are we comfortable with our financial exposure?

Protective Measures

- What safeguards are in place against risks?
- How do we detect and monitor threats

Response Readiness

- How prepared are we to respond and recover?
- Are our incident response plans effective?

Strategic Investment

- Where should we focus resources to reduce risk?
- Which investments yield the best risk mitigation return?

Competitive Positioning

- Are we keeping pace with competitors?

newera. TECHNOLOGY

In Cybersecurity, Risk is Our Business

"Risk. Risk is our business. That's what this starship is all about. That's why we're aboard her."

~ Captain James T. Kirk

In Cybersecurity, Risk is Our Business

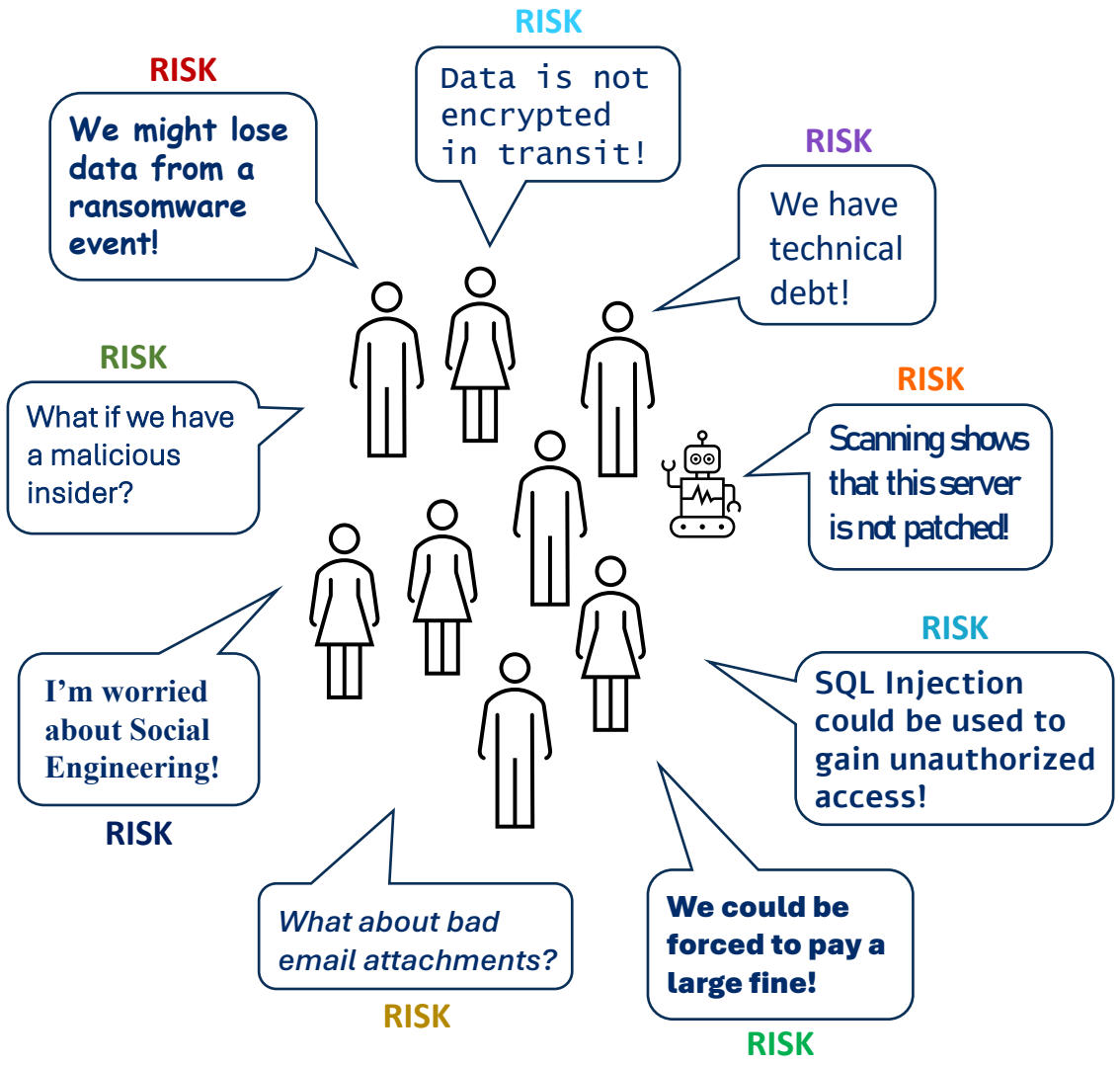
"Risk. Risk is our business. That's what this starship is all about. That's why we're aboard her."

~ Captain James T. Kirk

"You keep using that word. I do not think it means what you think it means."

~ Inigo Montoya

Making Sense of Observations



Language Reflects Environment

Inuit: Spoken in North American Arctic and subarctic regions; many words for *snow.*

Kriplyana: snow that looks blue in the early morning
Hiryla: snow in beards
Ontla: snow on objects
Intla: snow that has drifted indoors
Bluwid: snow that is shaken down from objects in the wind
Tlanid: snow that's shaken down and then mixes with sky-falling snow
Tlamo: snow that falls in large wet flakes.
Tlaslo: snow that falls slowly
Priyakli: snow that looks like it's falling upward
Kripya: snow that has melted and refrozen
Tlun: snow sparkling with moonlight
Aput: Snow on the ground
Qanik: Snow in the air, falling snow
Piqsirpoq: Drifted snow
Qimuqsuq: Snow drifted by the wind
Matsaaq: Wet or slushy snow
Pukak: Crystalline snow on the ground
Kanevvluk: Fine snow
Muruaneq: Soft, deep snow

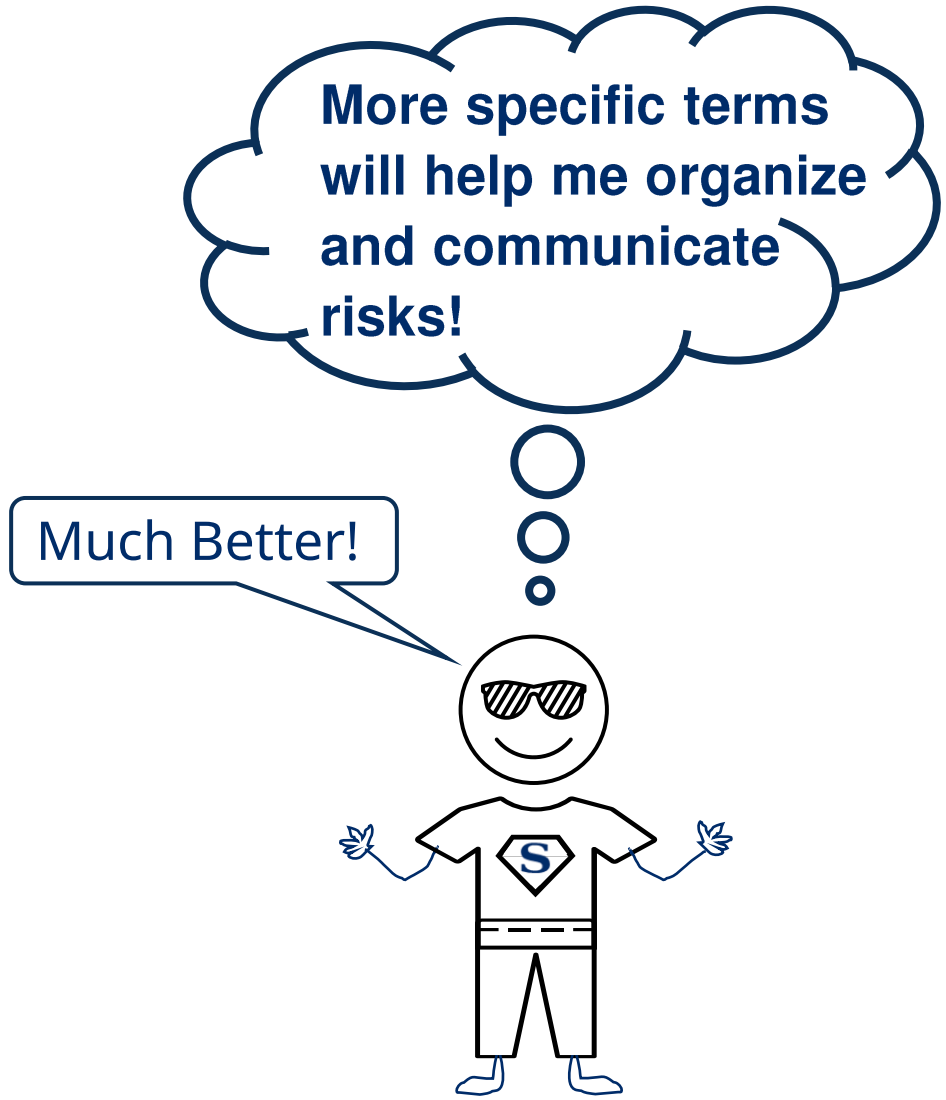
Language Reflects Environment

Inuit: Spoken in North American Arctic and subarctic regions; many words for *snow.*

Kriplyana: snow that looks blue in the early morning
Hiryla: snow in beards
Ontla: snow on objects
Intla: snow that has drifted indoors
Bluwid: snow that is shaken down from objects in the wind
Tlanid: snow that's shaken down and then mixes with sky-falling snow
Tlamo: snow that falls in large wet flakes.
Tlaslo: snow that falls slowly
Priyakli: snow that looks like it's falling upward
Kripya: snow that has melted and refrozen
Tlun: snow sparkling with moonlight
Aput: Snow on the ground
Qanik: Snow in the air, falling snow
Piqsirpoq: Drifted snow
Qimuqsuq: Snow drifted by the wind
Matsaaq: Wet or slushy snow
Pukak: Crystalline snow on the ground
Kanevvluk: Fine snow
Muruaneq: Soft, deep snow

Languages in tropical or arid regions: May not have a specific word for snow -- *because the region never experiences it*.

Making Sense of Observations

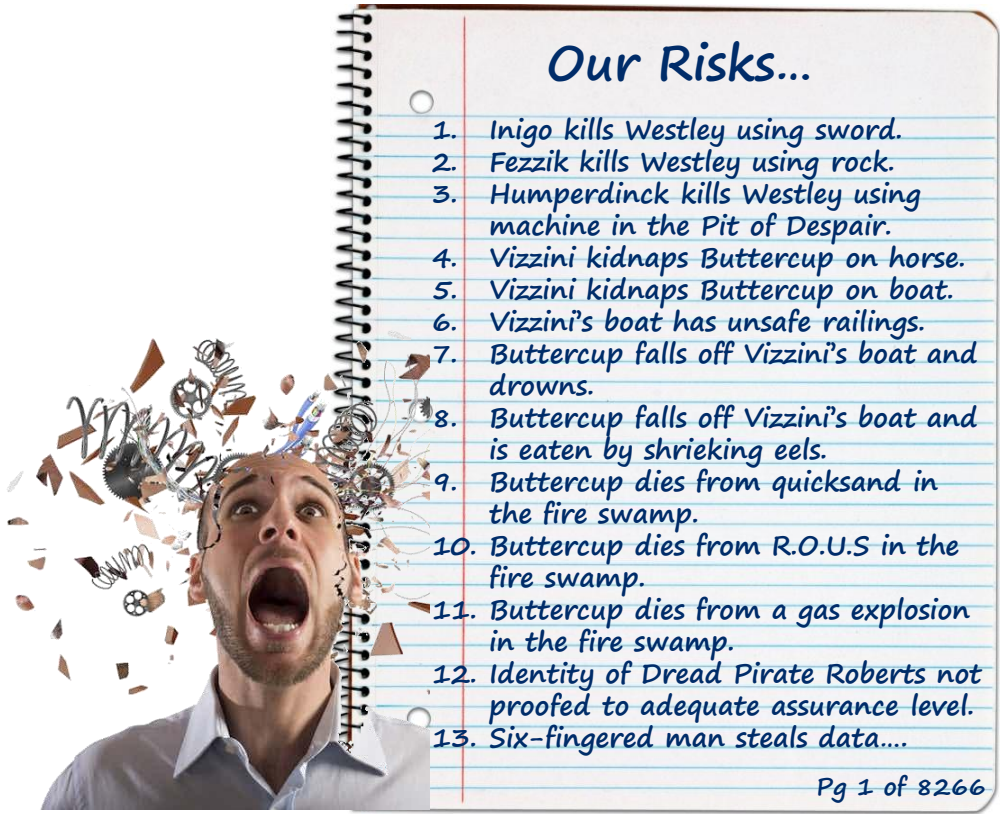


Breaking Down Risk – But How?

If we don't break it down <u>enough</u>...

... we don't get actionable information.

But if we break it down <u>too much</u>...

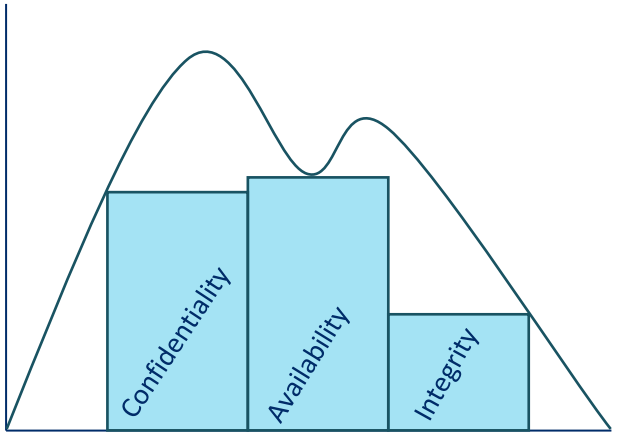


... we generate noise, making risk management unwieldy and less effective.

The 'Calculus' of Risk Management

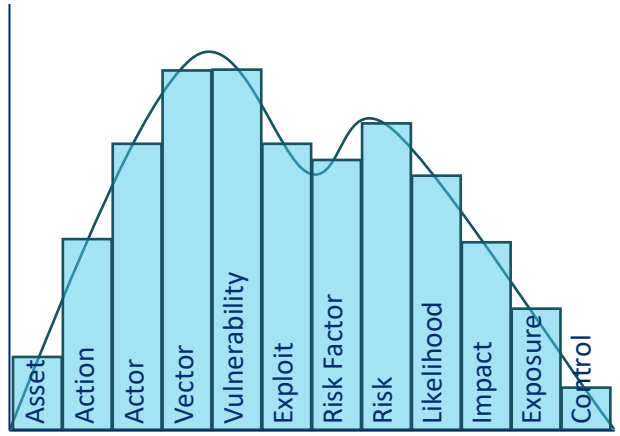
In calculus we can solve difficult problems by breaking them down into smaller, manageable parts (differentiation) and then re-assembling them (integration) to find the overall solution. Our approach to risk management involves dissecting risk into narrowly-defined concepts. By understanding the nuances of each, we can assemble these elements into a practical and effective methodology for managing the risk register.

Not Enough Detail



Noisy & Unmanageable

Just Right!



VERIS Primer

The Vocabulary for Event Recording and Incident Sharing (VERIS) is a set of terms designed to provide a common language for describing security incidents in a structured and repeatable manner. The annual Verizon Data Breach Investigations Report (DBIR) uses VERIS to describe cybersecurity incidents and trends. We're focusing on the seven VERIS THREAT ACTIONS, which we will subsequently use to help uncover related risks. The threat actions are:

Malware: Malware is any malicious software, script, or code run on a device that alters its state or function without the owner's informed consent. E.g., viruses, worms, spyware, keyloggers, backdoors, etc.

Hacking: Attempts to intentionally access or harm information assets without (or exceeding) authorization by circumventing or thwarting logical security mechanisms. Includes brute force, SQL injection, cryptanalysis, denial of service attacks, etc.

Social: Social tactics employ deception, manipulation, and intimidation to exploit the human element, or users, of information assets. Includes pretexting, phishing, blackmail, threats, scams, etc.

Misuse: The use of entrusted organizational resources or privileges for any purpose or manner contrary to that which was intended.

Physical: Deliberate actions that involve proximity, possession, or force. Includes theft, tampering, snooping, sabotage, local device access, assault, etc.

Error: Anything done (or left undone) incorrectly or inadvertently. Includes omissions, misconfigurations, programming errors, trips and spills, malfunctions, etc.

Environmental: Natural events such as earthquakes and floods, plus hazards associated with the immediate environment or infrastructure in which assets are located. Includes power failures, electrical interference, pipe leaks, and atmospheric conditions.

See https://verisframework.org/

Terminology: Assets, Threats, & Exploits

Asset

The data, personnel, devices, systems, and facilities that enable the organization's business purposes.

- *Laptops*
- *Servers*
- *Mobile Phones*
- *Network Hardware*
- *Databases*
- *Cloud Storage*
- *Anything of Value*

Threat Actor

An individual or group that can pose a threat or instigate a risk that could cause harm.

- *Activist*
- *Nation-state*
- *Organized Crime*
- *Force majeure*
- *Malicious Insider*

Threat Action

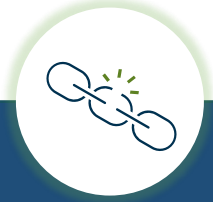
What the threat actors can do to cause or contribute to an incident.

- *Malware*
- *Hacking*
- *Social*
- *Misuse*
- *Physical*
- *Error*
- *Environmental*

Attack Vector

The intent and method targeted at the intentional exploitation of a vulnerability.

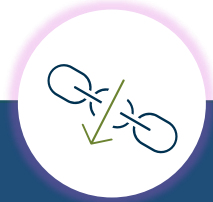
- *Email Link*
- *Email Attachment*
- *VPN*
- *Physical Access*
- *Phone / SMS*
- *Backdoor*
- *Carelessness*



Vulnerability

A weakness in an information system that can be exploited by a Threat Actor.

- *Unpatched OS*
- *Misconfiguration*
- *Non-Secure Code*
- *Zero-Day*



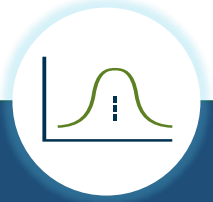
Exploit (n.)

Code or method that takes advantage of a vulnerability in a system, application, or network.

- *Cross-Site Scripting*
- *SQL Injection*
- *Auth Bypass*
- *Pass-the-hash*

VERIS (Adapted) — NIST CSRC (Adapted) — Wikipedia

Terminology: Estimating & Treating Risk



Risk Factor

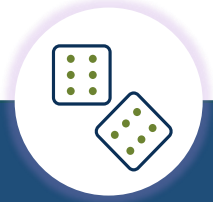
A condition or circumstance that influences the likelihood or impact of a risk eventuating.

- *Technical Debt*
- *Lack of Resources*
- *Governance Gaps*
- *Inadequate Training*
- *Market Volatility*

Risk

The potential loss of integrity, availability, or confidentiality of information or information systems.

- *Account Compromise*
- *Data Compromise*
- *Application Comp.*
- *System Compromise*
- *Infrastructure Comp.*
- *Financial Compromise*
- *Response Compromise*



Likelihood

The potential for loss or damage when a Threat Actor exploits a vulnerability.

- *Very Unlikely*
- *Somewhat Unlikely*
- *Possible*
- *Somewhat Likely*
- *Very Likely*

or

- *Percentage*

Loss (Impact)

The damage that can be done to business operations when a Threat Actor exploits a vulnerability.

- *Productivity*
- *Response*
- *Replacement*
- *Fines & Judgements*
- *Competitive*
- *Reputation*

Risk Exposure

Extent to which an organization is subject to a risk. ***'Likelihood x Impact'.***

- *Critical*
- *High*
- *Medium*
- *Low*
- *Nominal*

or

- *Loss Expectancy / yr*

Control (n.)

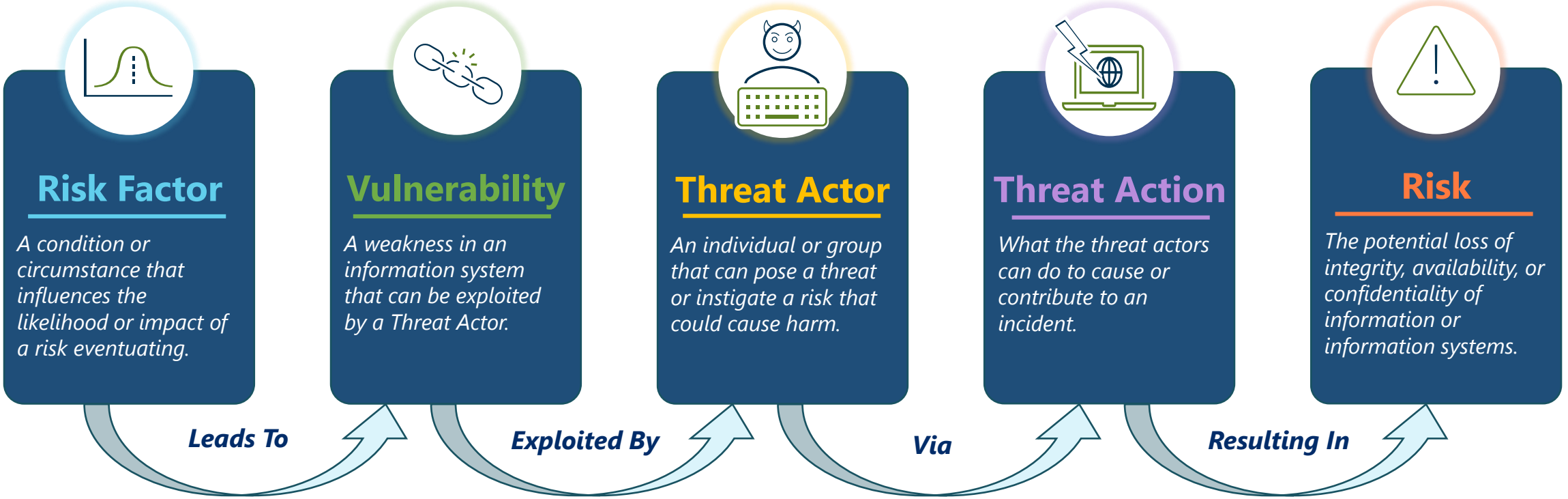
A Physical, Technical, or Administrative safeguard that addresses a threat or vulnerability.

- *Policies*
- *Anti-virus*
- *Encryption*
- *Backups*
- *Firewalls*
- *Email Filtering*
- *Access Controls*

ISACA (Adapted) — NIST CRISC (Adapted) — FAIR (Adapted) — NIST CSRC (Adapted)

Risk Factors and Risk Chains

A Risk Factor may drive multiple risks. A Risk Chain illustrates the sequence of how a Risk Factor leads to a vulnerability, which can be exploited by a threat actor via a threat action, resulting in a risk that may impact the organization.



- Shows the causal relationship between different elements of risk.
- Helps to understand how risks originate and propagate.
- Aids in identifying where safeguards can be most effective.

Our Goals Are To:

Understand the Purpose of a Risk Register

Leverage the VERIS threat actions to understand what organizational risks should be recorded

Contents

The Purpose of a Risk Register

A Risk Register is a centralized repository that documents identified risks, their assessment in terms of likelihood and impact, and the actions planned to treat them. It serves as a dynamic tool for tracking risks throughout their lifecycle, enabling organizations to systematically understand and address potential threats to their objectives, assets, and operations.

X What a Risk Register IS NOT:

- **The MITRE ATT&CK Framework**
  - It's not a catalog of adversary tactics and techniques used for cyber threat intelligence.
  - It’s not the cyber kill chain.
  - It’s not a basis for Threat Hunting.
- **A List of Vulnerabilities**
  - It's not a vulnerability reporting or management tool.
  - It’s not the national CVE Database.
- **A Capability Map**
  - It's not a representation of the organization's capabilities, processes, or competencies.
- **A Controls Framework**
  - It's not a list of security controls or compliance requirements like HIPAA, NY-DFS, NIST CSF, ISO 27001, etc..

✓ What a Risk Register IS:

- **A Structured Risk Management Tool**
  - It helps identify, estimate, and prioritize risks.
  - It can be used to record risk treatment plans (mitigation, avoidance, transfer, acceptance) and track progress.
- **A Communication Aid**
  - It enhances transparency and supports decision-making.
- **A Dynamic Document**
  - It should be updated regularly to reflect current risks.
- **Aligned with Business Objectives**
  - It supports risk management goals and compliance requirements.
  - It reflects the organization's risk appetite.

Risk Categories

At a high level, what are your organization's cybersecurity risks – the things that could affect the *Confidentiality*, *Integrity*, and the *Availability* of your information assets? Consider:

Credential Compromise: The loss of confidentiality or loss of control of one or more authentication factors. Includes Standard, Privileged, and Non-Human identities.

Data Compromise: The loss of Confidentiality, Integrity, or Availability of information. Includes data exposure and exfiltration, unauthorized alteration, and loss of access by authorized users.

Application Compromise: Adverse events including tampering or unauthorized access to source code, applications, APIs, and API gateways.

System Compromise: Lack of system stability or integrity, or interference with access to organizational systems.

Infrastructure Compromise: The Loss of the availability or integrity of the services that support or enable organizational systems. Includes outages of network and utilities.

Third-Party Compromise: The interruption of products or services provided by a partner, supplier, or vendor for any reason.

Financial Compromise: Events which directly affect the organization's costs or cause a financial loss.

Response Compromise: The degradation or loss of the organization's ability to detect anomalous conditions and take appropriate action.

Methodology

Use the VERIS threat actions to understand and review the undesirable events that could affect your organization's assets, ***to your desired level of detail.*** *See https://verisframework.org/enums.html#section-actions.* Consider the **VARIETY** and **VECTOR** for each action. For example:

ACTION.MALWARE.VARIETY

ADWARE: ADWARE
BACKDOOR: BACKDOOR (ENABLE REMOTE ACCESS)
BRUTE FORCE: BRUTE FORCE ATTACK
CAPTURE APP DATA: CAPTURE DATA FROM APPLICATION OR SYSTEM PROCESS
CAPTURE STORED DATA: CAPTURE DATA STORED ON SYSTEM DISK
CLIENT-SIDE ATTACK: CLIENT-SIDE OR BROWSER ATTACK (E.G., REDIRECTION, XSS, MITB)
CLICK FRAUD: CLICK FRAUD OR BITCOIN MINING
C2: COMMAND AND CONTROL (C2)
DESTROY DATA: DESTROY OR CORRUPT STORED DATA
DISABLE CONTROLS: DISABLE OR INTERFERE WITH SECURITY CONTROLS
DOS: DENIAL OF SERVICE ATTACK
DOWNLOADER: DOWNLOADER (PULL UPDATES OR OTHER MALWARE)
EXPLOIT VULN: EXPLOIT VULNERABILITY IN CODE (VS MISCONFIG OR WEAKNESS)
EXPORT DATA: EXPORT DATA TO ANOTHER SITE OR SYSTEM
PACKET SNIFFER: PACKET SNIFFER (CAPTURE DATA FROM NETWORK)
PASSWORD DUMPER: PASSWORD DUMPER (EXTRACT CREDENTIAL HASHES)
RAM SCRAPER: RAM SCRAPER OR MEMORY PARSER (CAPTURE DATA FROM VOLATILE MEMORY)
RANSOMWARE: RANSOMWARE (ENCRYPT OR SEIZE STORED DATA)
ROOTKIT: ROOTKIT (MAINTAIN LOCAL PRIVILEGES AND STEALTH)
SCAN NETWORK: SCAN OR FOOTPRINT NETWORK
SPAM: SEND SPAM
SPYWARE/KEYLOGGER: SPYWARE, KEYLOGGER OR FORM-GRABBER (CAPTURE USER INPUT OR ACTIVITY)
SQL INJECTION: SQL INJECTION ATTACK
ADMINWARE: SYSTEM OR NETWORK UTILITIES (E.G., PSTOOLS, NETCAT)
WORM: WORM (PROPAGATE TO OTHER SYSTEMS OR DEVICES)
UNKNOWN: UNKNOWN
OTHER: OTHER

ACTION.MALWARE.VECTOR

DIRECT INSTALL: DIRECTLY INSTALLED OR INSERTED BY THREAT AGENT (AFTER SYSTEM ACCESS)
DOWNLOAD BY MALWARE: DOWNLOADED AND INSTALLED BY LOCAL MALWARE
EMAIL AUTOEXECUTE: EMAIL VIA AUTOMATIC EXECUTION
EMAIL LINK: EMAIL VIA EMBEDDED LINK
EMAIL ATTACHMENT: EMAIL VIA USER-EXECUTED ATTACHMENT
INSTANT MESSAGING: INSTANT MESSAGING
NETWORK PROPAGATION: NETWORK PROPAGATION
REMOTE INJECTION: REMOTELY INJECTED BY AGENT (I.E. VIA SQLI)
REMOVABLE MEDIA: REMOVABLE STORAGE MEDIA OR DEVICES
WEB DRIVE-BY: WEB VIA AUTO-EXECUTED OR "DRIVE-BY" INFECTION
WEB DOWNLOAD: WEB VIA USER-EXECUTED OR DOWNLOADED CONTENT
UNKNOWN: UNKNOWN
OTHER: OTHER

It is not necessary to record a risk for every VERIS Variety and Vector! Consider threat actions that would be particularly impactful, and where your organization may be lacking adequate controls.

Map Threat Actions & Risks to an Optimal Level of Detail

Risk Category \ VERIS Threat Actions ->	**Malware** - Commodity - Ransomware	**Hacking** - Cred Stuffing - Vuln Exploit	**Social** - Phish / SMSish - Soc Networking	**Misuse** - Policy Violation - Malicious Insider	**Physical** - Control Bypass - B&E	**Error** - Misconfiguration - Accident	**Environmental** - Weather - Pandemic
Credential Compromise - Standard Account - Privileged Account - Non-human Account	• Trojan / Keylogger	• Brute Force • Unauthorized Acct Creation	• Phishing • Cred Harvesting • Impersonation to Helpdesk	• Weak Password • Privilege Misuse • Password Shared	• Tailgating • Burglary • Rogue Device	• Password on a Sticky Note • Svc Acct Allows Interactive Login	X
Data Compromise - Confidentiality (Expose / Exfil) - Integrity (Alter) - Availability (Delete / Encrypt)	• Ransomware • Data Stealer	• Eavesdropping • DoS Attack • Website Defacement	• Information Disclosure	• Unauthorized Change • Privilege Misuse	• Decom Hardware Exposure • Stolen Asset Exfil • Rogue Device Exfil	• Cloud Storage Data Exposure • Accidental Deletion / Change	X
Application Compromise - API / Gateway Compromise - Application Compromise	• Infected App	• Exploit API Vuln • Exploit App Vuln	• Impersonation of Authorized User	• Application Misuse • Exceed Rate Limit	X	• Bug in Application • WAF Misconfig	X
System Compromise - Availability - Lateral Movement	• Malware • Ransomware	• DoS Attack • Living off the Land	• Impersonation of System Admin	• Config Tampering • Unauthorized Tools	• Vandalism	• Access Control	• Fire • Flood
Infrastructure Compromise - Network Availability - Utility Outage	• Worm Propagation	• DDoS Attack • Router Exploited	• Impersonation of Network Admin	• Capacity Exceeded	• Bypass Facility Access Controls	• Backhoe Cuts Cables • Non-redundant	• Electrical Outage • WFH Capacity Insufficient
Third-Party Compromise - Cybersecurity Incident - Supply Chain Issues	• Vendor / Partner Malware Event • Spreads to Org	• Hacked via a Partner	• Impersonation of Third-Party Contact	• Partner Misuse of Auth Access	• Supply Chain Tampering	• Misconfiguration Affects Other Users	• Supply Chain Interruption • Facility Damage
Financial Compromise - Theft / Fraud - Judgements - Revenue Loss	• Banking Trojan • Crypto Miner	• Unauthorized Account / Routing Change	• Business Email Comp. (BEC) • Other Fraud	• Unauthorized Purchases • Other Fraud	• Theft of Assets	• Payment Error • Fines Due to Non-Compliance	• Damage to Facilities & Assets
Response Compromise - Increased Response Cost - Increased Response Time	• Malware Evades Defenses	• Hacker Evades Responders	• Hacker Tricks Responders	• Improper Use of Response Tools	X	• Lack of Backup • Unprepared • Slow Response	• Reduced Resources

Generative AI Characteristics and Capabilities

What Does Your Organization Need to Know?

- It can produce a variety of novel content, such as images, video, music, speech, text, software code and product designs.
- GenAI is different than machine learning because GenAI can "teach itself" by ingesting "training" data *(Machine Learning needs to be told what to do every time)*.
- GenAI is conversational (you can ask natural language questions and GenAI can interpret it).
- GenAI can provide simple productivity gains (e.g., summarizing data quickly to get faster insights or producing technical documentation and code as a baseline, etc.) – More complex use cases can be identified after simpler use cases like content generation.
- Humans must always be in the loop (GenAI can "hallucinate") and therefore, governance and data integrity guardrails must be set.

Generative AI Risks

What Risks Does Your Organization Need to Address?

59% of employees use unapproved AI tools at work

Source: Cybernews.com

- Lack of Transparency: Generative AI and ChatGPT models are unpredictable, and not even the companies behind them always understand everything about how they work.
- Accuracy: Generative AI systems sometimes produce inaccurate and fabricated answers. Assess all outputs for accuracy, appropriateness and actual usefulness before relying on or publicly distributing information.
- Bias: You need policies or controls in place to detect biased outputs and deal with them in a manner consistent with company policy and any relevant legal requirements.
- Intellectual property (IP) and copyright: There are currently no verifiable data governance and protection assurances regarding confidential enterprise information. Users should assume that any data or queries they enter into services like ChatGPT will become public information.
- Cybersecurity and Fraud: Enterprises must prepare for malicious actors' use of generative AI systems for cyber and fraud attacks, such as those that use deep fakes for social engineering of personnel, and ensure mitigating controls are put in place. Confer with your cyber-insurance provider to verify the degree to which your existing policy covers AI-related breaches.
- Sustainability: Generative AI uses significant amounts of electricity. Choose vendors that reduce power consumption and leverage high-quality renewable energy to mitigate the impact on your sustainability goals.

Phishing attacks increased by 1,265% driven by growth of Gen AI

Source: SentinelOne

Q&A

Questions?

Thank You

newera.
TECHNOLOGY

Appendix A: Risk Management Lifecycle & Sources

Our Goals Are To:

Understand the Risk Management Lifecycle

Understand how the organization periodically gathers information about risk

Contents

The Risk Management Lifecycle

Sources of Risk Information (Examples)

Annual	Description	Identify	Analyze & Estimate	Prioritize & Treat	Monitor	Report
Risk & IT Controls Assessment	Attestation-based assessment aligned to NIST Cybersecurity Framework 2.0 sub-categories.	Interview SMEs across multiple stakeholder groups to capture domain-specific safeguards.	External assessor estimates likelihood and Impact of realized risk, based on inherent risk and any controls gaps, and provides recommendations for remediation.	Information Security leadership considers organizational risk tolerance & other identified risks, determines treatment strategy, and drives remediation projects.	Metrics, including KRIs if appropriate, are implemented. Risk register is updated to reflect residual risk.	Information Security leadership reports risk posture to Audit Committee and Board of Directors.

Bi-Annual	Description	Identify	Analyze & Estimate	Prioritize & Treat	Monitor	Report
Penetration Testing	Test of technical controls by an external service provider.	Automated and Manual penetration testing to identify controls gaps.	Service provider estimates severity of each finding.	Information Security leadership determines risk treatment.	Repeat / subsequent testing verifies that gaps are remediated.	Findings are remediated per policy or documented in the IT Risk Register.
Tabletop Exercise	Cyber Incident Response Plan (CIRP) is tested with IT and Information Security teams twice per year and includes technical and executive audiences.	Simulate a cyber-attack and identify readiness gaps.	Session leader and participants estimate severity of any findings.	Information Security leadership determines risk treatment.	Subsequent testing verifies that gaps are remediated.	Findings are remediated per policy or documented in the IT Risk Register.
DR Failover Test	Business Continuity and Disaster Recovery teams execute a DR failover test, including IT and Business Functions.	Test IT and business readiness to meet recovery objectives.	Dir, Business Resiliency grades each test on issues and meeting RTO.	Business Resiliency and Disaster Recovery teams prioritize.	Subsequent testing verifies that gaps are remediated.	Findings are remediated per policy or documented in the IT Risk Register.

Sources of Risk Information (Examples)

Quarterly	Description	Identify	Analyze & Estimate	Prioritize & Treat	Monitor	Report
Key Controls Review	Key controls are reviewed quarterly by the control owners, facilitated by the Sr. IT Risk Analyst.	Identified key controls are validated for gaps / effectiveness.	Any controls gaps and associated risks are documented.	Newly identified risks are prioritized for treatment.	Effectiveness of controls implemented since last review is evaluated.	Meeting minutes are published to stakeholders and IT leadership.

Bi-Weekly	Description	Identify	Analyze & Estimate	Prioritize & Treat	Monitor	Report
Risk Review	Consumption of risk information from the business. Review, rate, and refine risks captured in Risk Register. Facilitated by the Sr. IT Risk Analyst.	SMEs review and validate documented risks and identify new risks to record.	Sr. IT Security Risk Analyst updates Risk Register.	Newly identified risks are prioritized for treatment.	Effectiveness of controls implemented since last review is evaluated.	Meeting minutes are published to stakeholders and IT leadership.

Weekly	Description	Identify	Analyze & Estimate	Prioritize & Treat	Monitor	Report
ServiceNow Discovery	Discovery finds computers, servers, printers, a variety of IP-enabled devices, and the applications that run on them.	Identifies known and unknown devices found on the network.	Updates Configuration Items (CIs) in CMDB. New CIs logged.	Existing CIs are updated.	Monitored by KPI process.	Discovery data reported weekly to engineering. (Escalated as needed.)

Sources of Risk Information (Examples)

Daily	Description	Identify	Analyze & Estimate	Prioritize & Treat	Monitor	Report
Threat & Vulnerability Analysis (TVA)	Daily meeting with business, IT, and Information Security stakeholders. Participants contribute any new threat intel from public, private, and internal sources.	Threat intelligence and vulnerability information sharing.	New threats and risks are analyzed for likelihood and impact; applicability of current controls.	Information Security leadership determines risk treatment.	Applicable controls effectiveness monitored by KPI process.	SOC team sends report to TVA stakeholders daily.

Continuous	Description	Identify	Analyze & Estimate	Prioritize & Treat	Monitor	Report
Endpoint Scanning	Vulnerability scanning is continuously conducted on organizational assets to discover deviations from standards (e.g., missing patches, misconfigurations).	Missing patches and vulnerability signatures are identified.	Scanning integrates CVSS scoring to estimate severity.	ITSM ticketing for small configuration issues.	Repeat / subsequent testing verifies that gaps are remediated.	Scan-generated reporting. Any significant risks are added to the IT Risk Register.

Appendix B: Resources and Further Reading

Resources & Further Reading

- Star Trek Original Series Set Tour:
  - https://startrektour.com/
  - https://www.youtube.com/watch?v=4ErkeFA-QWk
- Linguistic Relativity Hypothesis:
  - https://en.wikipedia.org/wiki/Linguistic_relativity
  - https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0151138
  - https://www.cmu.edu/news/stories/archives/2016/april/language-reflects-environment.html#:~:text=However%2C%20a%20new%20study%20published,talk%20about%20snow%20and%20ice
- VERIS – The Vocabulary for Event Reporting and Information Sharing:
  - https://verisframework.org/
- Verizon Data Breach Investigations Report
  - https://www.verizon.com/business/resources/reports/dbir/
- MITRE ATT&K:
  - https://attack.mitre.org/
- NIST – The National Institute of Standards and Technology:
  - https://csrc.nist.gov/
- ISACA - The Information Systems Audit and Control Association:
  - https://www.isaca.org/
- FAIR – Factor Analysis of Information Risk:
  - https://www.fairinstitute.org/
- News:
  - https://cybernews.com/ai-news/59-of-employees-use-unapproved-ai-tools-at-work-most-of-them-also-share-sensitive-data-with-them/
  - https://www.sentinelone.com/cybersecurity-101/cybersecurity/cyber-security-statistics/
- SecureBlu by New Era:
  - https://www.neweratech.com/us/security-services/