DeRISK Industrial

Cyber Risk Quantification and Management for ICS/OT Asset Owners

The Business Impact of Cyber Risk

Industrial organizations today are exposed to catastrophic cyber risk. As cyber attacks on operational technology (OT) networks grow in number and and complexity, so has their cost to critical infrastructure operators and stakeholders. In fact, cyber risk has ballooned to over $1 trillion dollars in cost; and only 1% of it is covered by insurance.

> Cyber risk has ballooned to over $1 trillion dollars in cost

In spite of the introduction of new cybersecurity and threat intelligence platforms that are built for Industrial Control System (ICS) environments, CISOs and industrial asset owners still find their critical infrastructure under attack with an increasing rate of success and cost to their organization. Ransomware targeting ICS and OT has grown faster than ransomware targeting IT, growing 500% since 2018. Clearly, the innovation rate of malicious attack techniques have outpaced cybersecurity innovation. Industrial organizations require more than security from cyber threats, they require resiliency.

Cyber risk quantification, as well as the management and remediation insights, allows asset owners to assess their cyber risk posture on a continuous basis and hedge their exposure. With the DeRISK Platform, DeNexus answers these questions better than anyone, enabling industrial organizations to manage and invest in their business wisely.

Introducing DeRISK Industrial

The DeRISK Platform is purpose-built for the CISO, CRO and CFO in-mind, located in a FedRAMP certified infrastructure. DeRISK leverages operational asset data-flows, combined with contextual information and threat intelligence sourced from the DeNexus Knowledge Center© data lake illustrated in figure 1.

> Identify, quantify, mitigate and hedge cyber risk exposure.

DeRISK Industrial Benefits

Value Your Cyber Risk
Know your financial risk associated with every cyber risk at all times to make the right capital allocations

Defend Your Operation
Build better cyber defense strategies with detailed posture assessments of your entire operation

Mitigate Risk Exposure
Leverage the DeNexus Knowledge Center for detailed attack-path mapping

ROI-based Cybersecurity
Measure the financial impact of different mitigations and optimize capital allocation

Leverage Intuitive Interfaces
Reduce cyber risk with hundreds of visualizations built for the industrial asset owner in mind

The DeRISK Platform empowers risk stakeholders to financially quantify the cyber risk that their company is incurring in real-time. Through the DeRISK UI, asset owners are armed with the main factors driving their incurred cyber risk, where in their infrastructure cyber risk is located and how cyber risk can be remediated. CISOs, CTOs, CFOs and all operational stakeholders are able to achieve a central, holistic assessment their cyber risk exposure to better document and measure results, performance and mitigation-related investments.
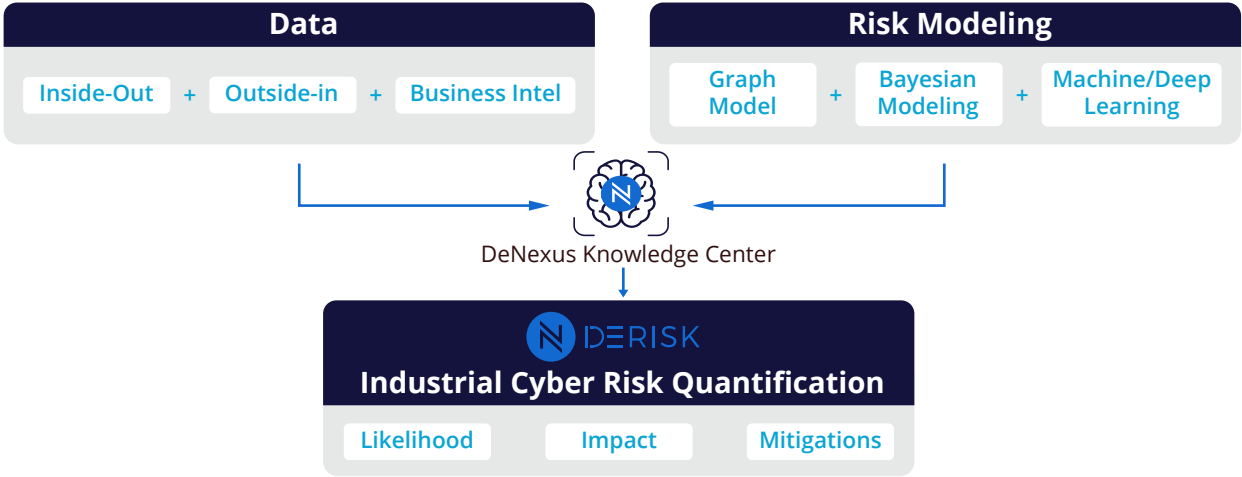
Data

Inside-Out + Outside-in + Business Intel

Risk Modeling

Graph Model + Bayesian Modeling + Machine/Deep Learning

DeNexus Knowledge Center

DERISK
Industrial Cyber Risk Quantification

Likelihood | Impact | Mitigations

Figure 1: DeNexus Knowledge Center powered by trusted data, probabilistic inference and machine learning
MITRE ATT&CK framework - CIS CSC - NIST CSF - ISA/IEC-62443-3-3 - ISO 27001 - FAIR

The DeRISK Solution

Comprehensive risk management for enterprise organizations, particularly for critical infrastructure and industrial environments, is dependent upon actioning operational and cybersecurity data. This is why the DeRisk Platform sources and aggregates data from all key operational areas, including intrusion detection, threat intelligence, contextual information and impact of successful breaches to provide dynamic and continuous cyber risk modeling via actionable dashboards that clearly visualizes the relationships between cyber-attack stages and the organization's specific infrastructure. The figure below illustrated how Initial Access Vectors (IAVs) are processed and analysed.
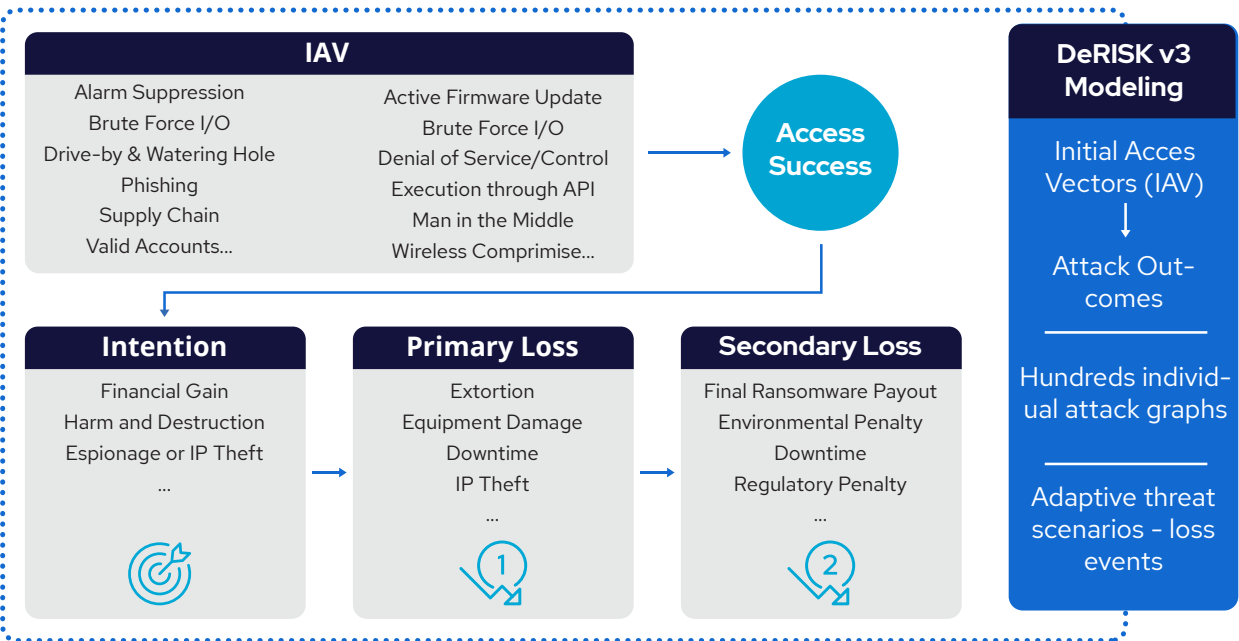
IAV

Alarm Suppression
Brute Force I/O
Drive-by & Watering Hole
Phishing
Supply Chain
Valid Accounts...

Active Firmware Update
Brute Force I/O
Denial of Service/Control
Execution through API
Man in the Middle
Wireless Comprimise...

Access Success

DeRISK v3 Modeling

Initial Acces Vectors (IAV)
↓
Attack Out-comes
____
Hundreds individual attack graphs
____
Adaptive threat scenarios - loss events

Intention

Financial Gain
Harm and Destruction
Espionage or IP Theft
...

Primary Loss

Extortion
Equipment Damage
Downtime
IP Theft
...

Secondary Loss

Final Ransomware Payout
Environmental Penalty
Downtime
Regulatory Penalty
...

Figure 2: Attack-Path mapping using the DeNexus probablistic modeling apporach

Leveraging the DeNexus Knowledge Center, DeRISK explores every possible attack path that attackers could take against a target, and estimates the probability of each attack path succeeding. Also, to quantify the impact of any loss event, the platform considers the impact of a primary loss plus any possible secondary losses of an event as well. The result is a powerful risk quantification and management tool-set, offered as-a-service, that arms risk and operational stakeholders with hundreds of actionable attack paths sourced from numerous diffferent threat variables that are reffered to as "nodes."

This method of probabilistic modeling allows industrial organizations to use DeRISK Industrial to calculate capital allocation against their risk exposure, establish loss reserving provisions for balance sheet purposes and enable compliance obligations for regulatory and rating agency purposes. In addition, DeRISK Industrial can be used to build cybersecurity strategies as well as build and hone cybersecurity solutions.

Key Capabilities and Functions

Attack-Path Mapping Interface

- End-to-end mapping of potential attack and ultimate loss event
- Hundreds of actionable attack paths for loss scenarios
- Access vectors with attacker intentions represented for improved cyber risk remediation and loss prevention action
- Bayesian probabilistic estimation of cyber-attack attempts and potential outcomes

Loss Event Quantification

- Comprehensive loss event classification derived from the Organization for Economic Co-operation and Development (OECD)
- Hierarchical analysis of primary and secondary financial losses
- Loss distribution composition providing a complete evaluation of risk

Dynamic Risk Aggregation

- Collection of asset and intrusions related information from host enviornment (inside-out risk sources)
- Threat intelligence informaton from public, private and proprietary data sources including supply-chain risks (outside-in risk sources)
- Multi-network bottom-up risk visibility

Risk Scenario Modeling

- Continuous detailed, dynamic vulnerability analysis with environmental and industry context
- Adaptive quantification engine to industry, sub-industry, facility features and their technology
- Historical data, risk quantification, what-if scenarios can be compared

DeRISK Solves the Money Questions for Industrial Asset Owners
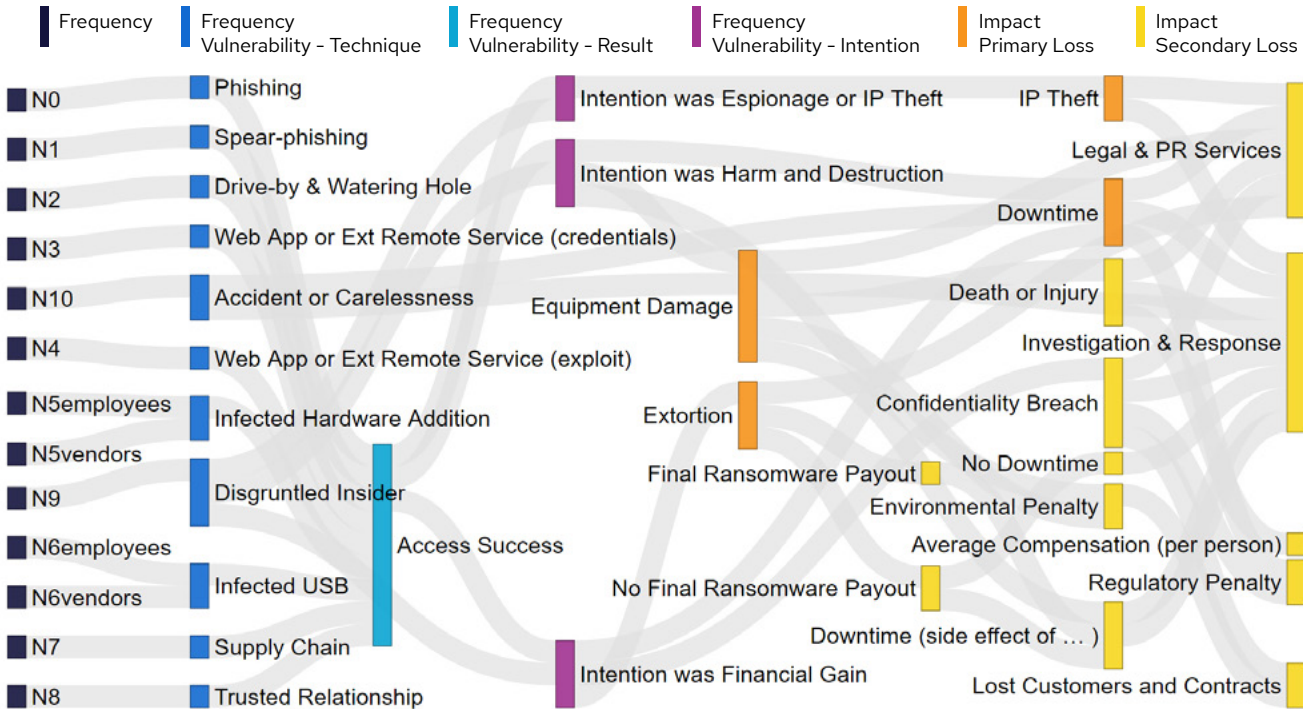

Figure 3: Attack-Path Mapping from IAV to Financial Impact

DeRISK combines empirical data and expert knowledge to provide Industrial organizations with:

Business Impact Valuation

- Quantifies cyber risk via the DeNexus modified and proprietary approach to the FAIR Framework using financial impact
- Provides insights based on Loss Event Frequency (LEF) and Loss Magnitude (LM) for detailed cyber risk analysis
- Classifies losses by Initial Access Vectors (IAV) to provide more granular information to cybersecurity stakeholders
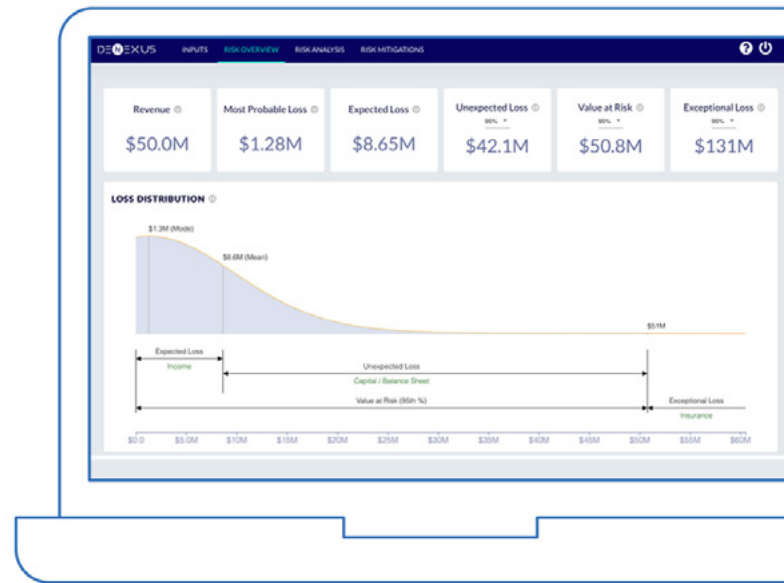
Defense Intelligence

- Standardizes cyber risk across a fleet of assets using MITRE Att&ck metrics
- Identifies potential attacker intention for improved cyber risk posture strategies
- Highlights optimum risk mitigation actions based on host ICS/OT network

Risk Mitigation

- Aligns Value at Risk (VaR) with potential cyber events
- Aggregates dynamic risk data to guide cybersecurity investments
- Visualizes analysis of multiple attack graphs representing specific threat scenarios and attack method

ROI-Based Risk Management

- Lowers operational costs by automating and optimizing risk assessments
- Improves cybersecurity investment and insurance selection with accurate, on-going cyber risk analysis

Actionable, Intuitive UI

- Prioritizes corrective actions according to urgency and impact of cyber events
- Assesses changes in cyber strategies and ROI's
- Intuitive data inputs for cyber security insurance evaluations

Quantify Cyber Risk. Save Money.

We are DeNexus

DeNexus is the leading provider of cyber risk modeling for ICS/OT organizations and global (re)insurers. Our platform empowers the industrial enterprise to quantify cyber risk exposure on a continuous, self-adaptive basis using the world's first evidence-based data analytics software and services. Our flagship solution offering is DeRISK, which is the world's first self-adaptive, cloud-based platform that uses evidence-based data to predict where and how breaches are likely to occur and what their business impact will be.

Fortune 500 companies, from power generation to manufacturing to other critical infrastructure, rely on DeNexus to understand their bespoke cybersecurity economics and optimize their risk-reduction ROI. Leverage DeNexus and our DeRISK Platform to make asset, vulnerable, configuration, operational anomaly, supply chain and cyber intrusion data work for you.

DENEXUS