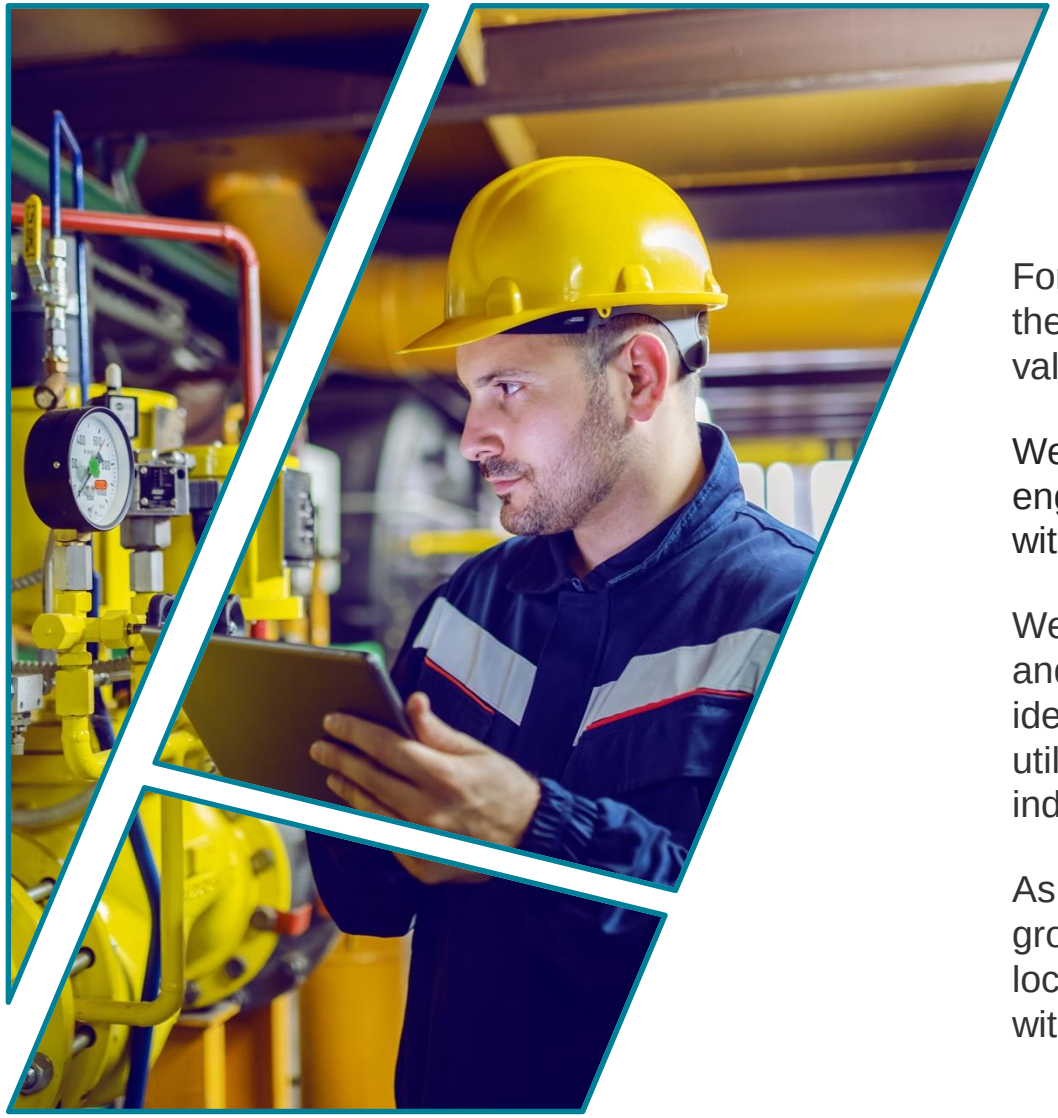
ENTRUST SOLUTIONS GROUP

Leveraging IM and PSMS to Assess & Mitigate Physical Threats

FGU Annual Conference

October 11, 2023

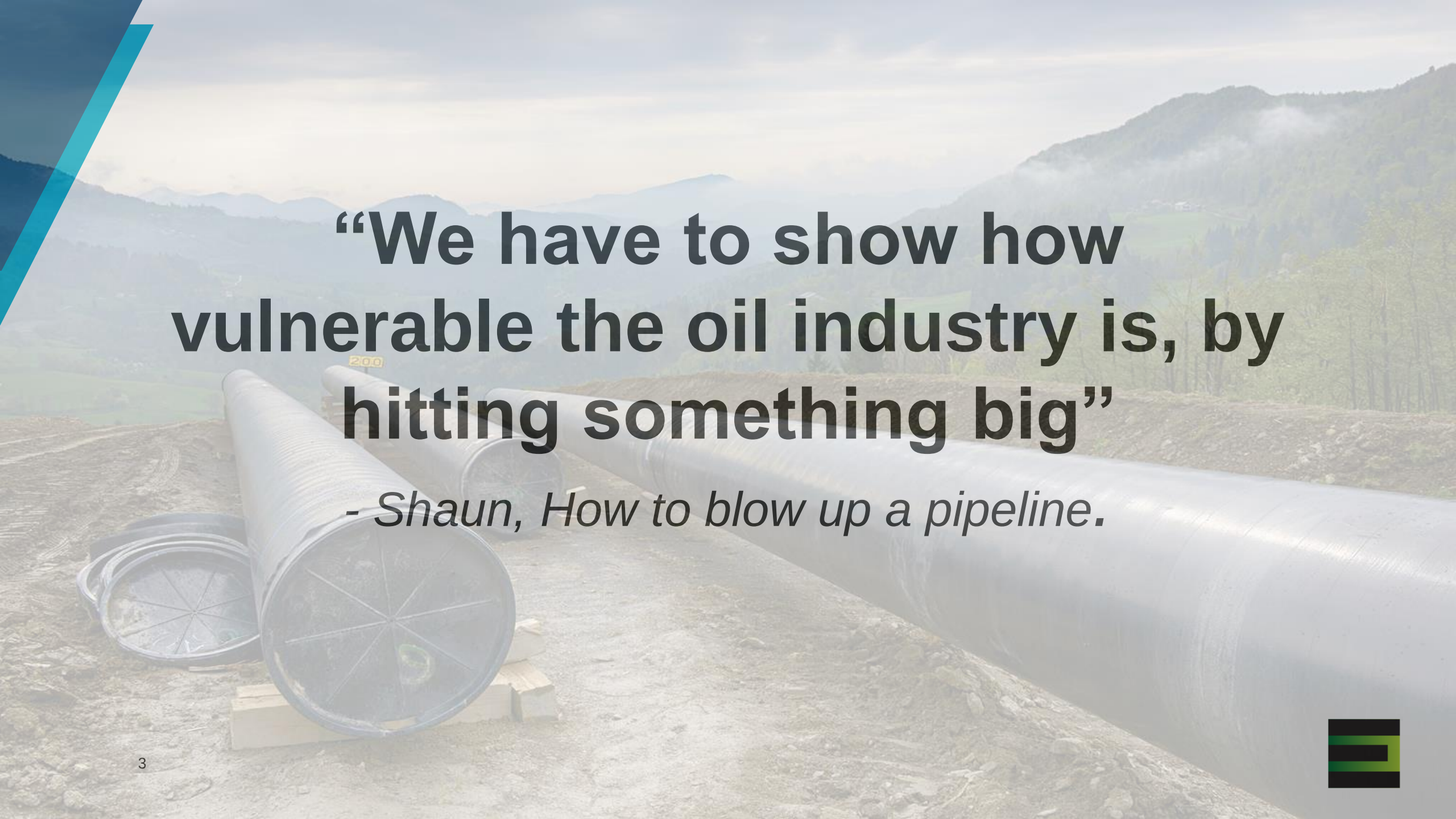


For over 20 years, businesses, people, and communities have relied on the employees of ENTRUST Solutions Group to protect their most valuable assets, infrastructure, and the projects that improve them.

We have embraced growing markets such as renewables, power engineering services, EV infrastructure, data analytics, and geospatial with cutting edge engineering, consulting, and automation services.

We offer valuable solutions to challenges faced by our clients, restore and expand infrastructures, enhance and streamline systems, and identify and record key assets for clients, including gas and electric utilities, telecommunication service providers, pipeline operators, and industrial companies.

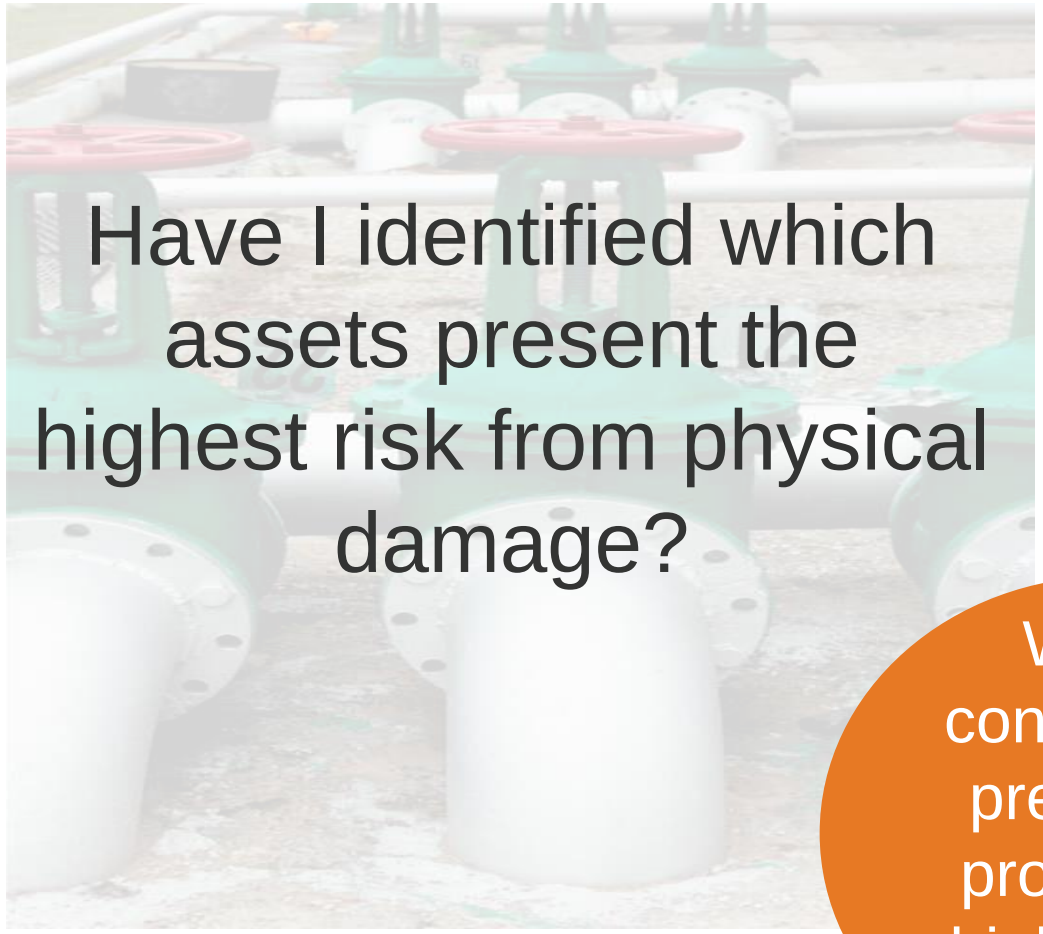
As one of the fastest-growing engineering firms in the country, we have grown from a single Midwest office to a national network of locations, which has only strengthened our commitment to serving with *excellence… from start to finish*.



“We have to show how vulnerable the oil industry is, by hitting something big”

- Shaun, How to blow up a pipeline.

Integrity Management



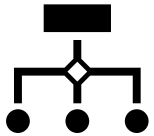
Have I identified which assets present the highest risk from physical damage?

Pipeline Safety Management System

Are my controls that mitigate the risks from physical damage effective?

Which controls are present to protect the highest risk assets?

Risk Management Processes

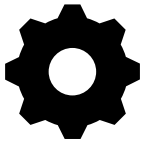


Enterprise Risk Management (ERM)

Focuses on executive-level, broad based corporate risks representing the entirety of business functions (operations, finance, IT, HR, etc.)

The ERM process is applied in a strategy setting and across the enterprise and is designed to identify potential events that may affect the entity and ensure that there is reasonable assurance regarding achievement of the entities' business objectives.

Low, ~12 Risk Items



Process, System or Event Based Risk Management (SMS)

Focuses on operational risks that are affected by the quality of controls related to a series of complex processes that make up the system

The SMS process is applied at an operational level and is designed to holistically evaluate a series of complex and interrelated processes, systems or events to identify and mitigate safety risks that could impact the workforce, assets or the public before an incident occurs.

Moderate, ~500 Risk Items

Asset Based Risk Management (TIMP, DIMP, SIMP, FIMP)

Focuses on operational risks that are a result of the performance of the assets within the operating system and the corresponding physical threats

The asset-based process is applied at an individual asset, system or class of assets and is designed to leverage detailed data about the asset, its performance and the effect of specific threats to drive an operational and engineering response to mitigate risk to a specific asset or asset class and ensure compliance with regulations.

High, ~X,000,000 Risk Items

Information is shared between the risk management processes to properly identify, assess, prioritize and respond to risks

Risk Evaluation Tools

Cause Analysis
- Cause and Effect Analysis
- Causal Mapping
- Design Safety Review
- Management Oversite & Risk Tree
- Fault Tree Analysis

Likelihood & Consequence Analysis
- Bow Tie Analysis
- Event Tree
- Fault Tree
- Failure Mode & Effects Analysis
- Hazard and Operability Study
- Job Risk Assessment
- Layers of Protection Analysis
- Preliminary Hazard Analysis
- Striped Bow-Tie Risk Assessment
- Structure What-if Technique

Controls Analysis
- **Bow Tie Analysis**
- Design Safety Review
- Failure Mode and Effects Analysis
- Hazard Analysis and Critical Control Points
- Hazard and Operability Study
- Layers of Protection Analysis
- Stiped Bow Tie Risk Assessment
- Structured What-if Technique

API 1173's primary focus is on the assessment and improvement of operational controls to mitigate risk.

Integrity Management programs are controls to mitigate risks identified in your PSMS

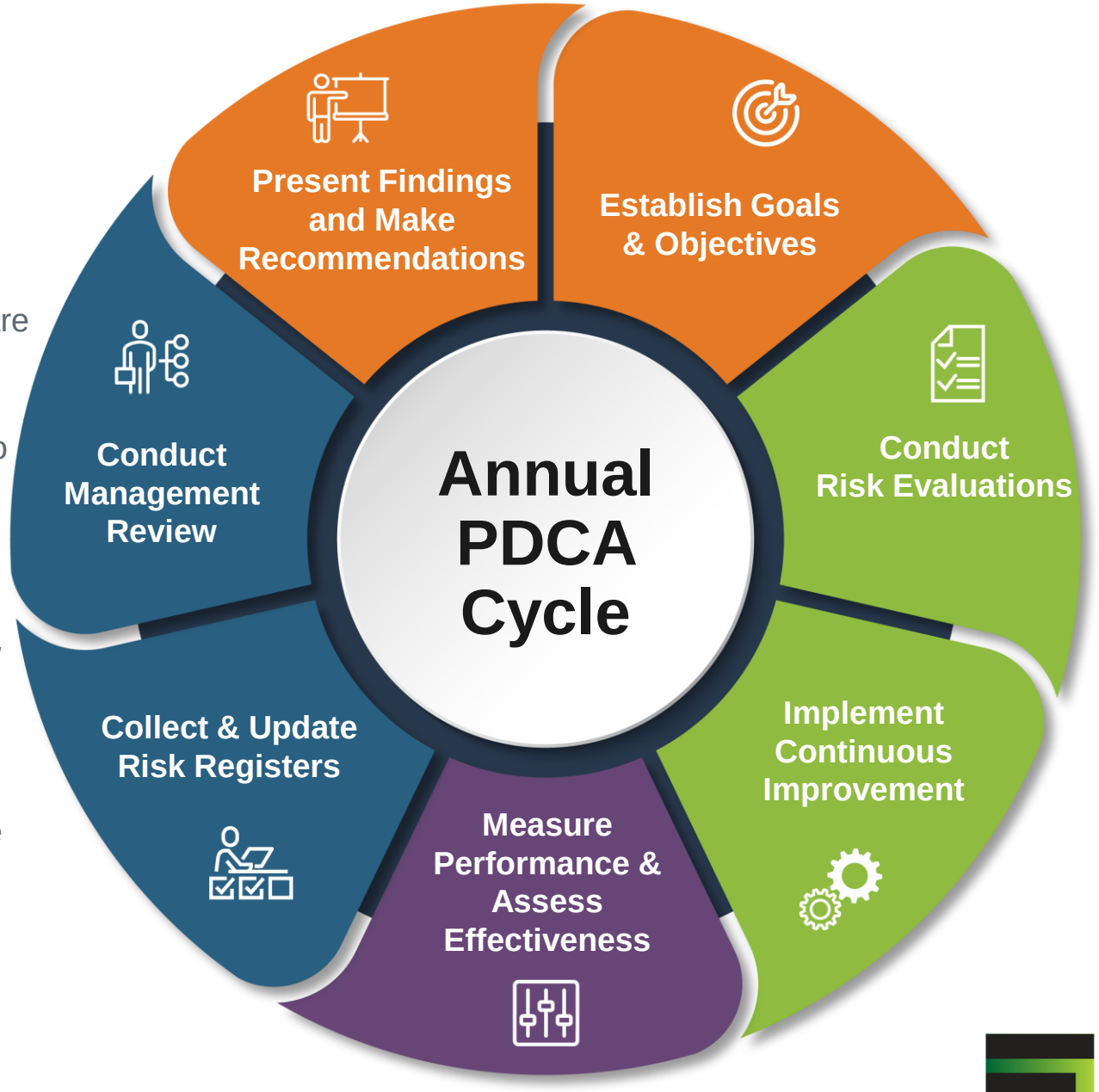
Implementing risk mitigations through your PSMS are preventive and mitigative measures to mitigate risks to assets identified by your Integrity Management programs.

ROUTINE & INTENTIONAL RISK REDUCTION

- Do our IM models assess physical threats from intentional acts to cause catastrophic harm?
- Are our P&M measures sufficient to reveal and mitigate risks from intentional acts to cause catastrophic harm?
- Do our control systems adequately monitor the pipeline system and offer the ability to immediately respond?
- Will our physical controls function as designed when the time comes?
- Have we evaluated the effectiveness of all controls that can prevent such an incident?
- Are we testing the effectiveness of those controls and are we measuring and monitoring the controls routinely.
- Have we proactively engaged our stakeholders to assess the risks and mitigations?
- Are our stakeholders ready to respond when the time comes?

Exercise PDCA

- Assess the pipeline assets or facilities and determine areas of highest risk.
- Identify controls specific to each asset or facility that are intended to prevent such a risk from occurring.
- Assess the effectiveness and identify improvements to controls.
- Implement the improved controls.
- Conduct QA/QC assessments of the existing and new controls.
- Leverage the data collected as part of the QA/QC process to identify where additional improvements are needed.
- Start the process all over again.



- Jim Francis
- Vice President - SMS Consulting
- jfrancis@entrustsol.com
- 812-305-2054

ACUMEN

FGU Annual Meeting

Industry Threats Panel

October 11, 2023

Florida GAS UTILITY

Cyber Security Presentation & Discussion

- Introductions
- The Cyber Security Threat Landscape for Utilities
- How to Address the Threat Landscape

Overview of Acumen

ACUMEN

We help our clients to maintain reliable operations, meet regulatory requirements, manage efficiencies, manage risk, and lower costs.

Acumen provides professional engineering, technical and management solutions

600+

Served over 600 utilities and municipal clients since 1984

Long standing success assisting public utilities with their cybersecurity challenges.

The Cyber Security Threat Landscape For Utilities

Cyber Security Threat Landscape

Vulnerability of Connecticut Utilities

Connecticut Utilities Regulatory Authority stated that electric, gas and water companies are increasingly vulnerable to cyberattacks, and that the array and **sophistication of cybersecurity threats is increasing** every year [1].

Urgent Warnings for Critical Infrastructure Providers

U.S. federal and international authorities have issued urgent warnings to critical infrastructure providers to take precautions against potential retaliatory cyberattacks from alleged **Russian state actors and criminal cyber groups** [2].

Escalating Cyberattacks on Energy Infrastructure

The quantity of **cyberattacks on energy infrastructure has increased substantially**, magnifying organizations' need to protect against cyberthreats [3]

[1] Report: Cyber Threats Against Utilities Grow in Complexity (govtech.com)

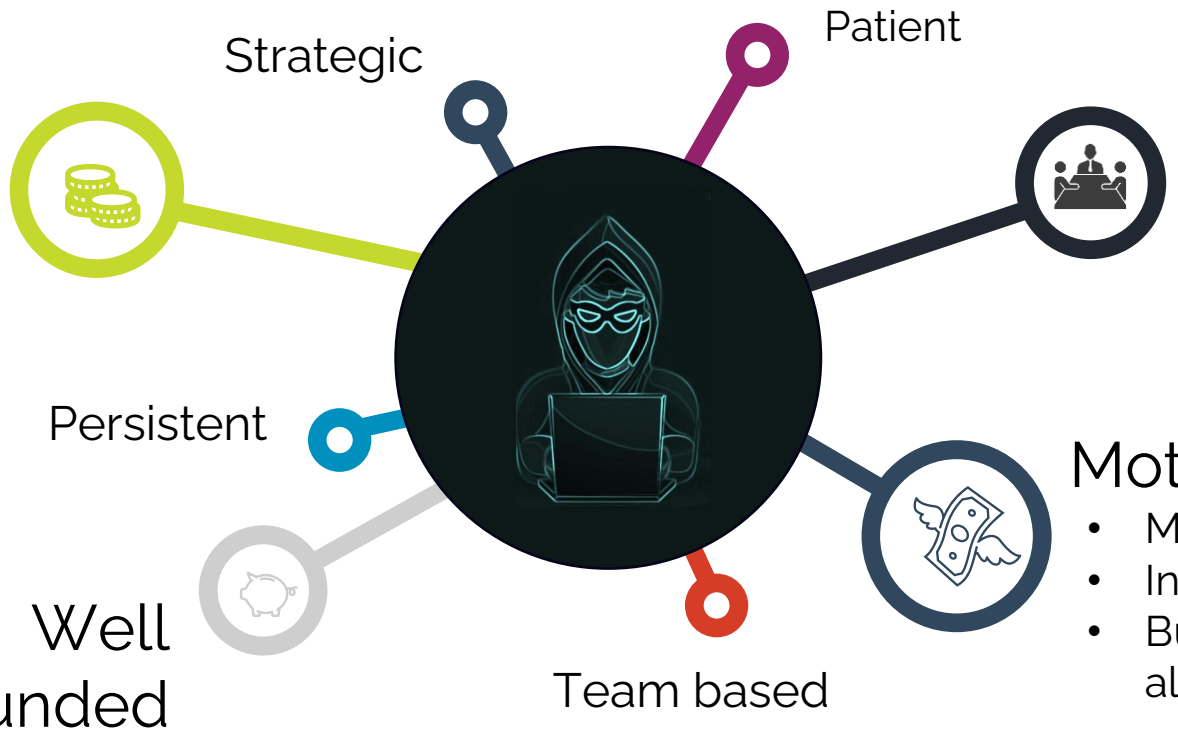
[2] Cyber agencies renew warnings of Russia-linked threats against industrial targets | Cybersecurity Dive

[3] Risks and Cybersecurity in the Energy Sector | Deloitte US

The Modern Hacker

Prime adversaries to Utilities:

- State Sponsored Actors
- Hacktivists
- Organized Crime – the adversary of most concern!



- Highly skilled technically
- Well trained

Motivated by:

- Money
- Influence
- But increasingly it's really all about the money

Ransomware

Source: https://www.utilitydive.com/news/ransomware-is-a-major-threat-to-smaller-utilities-manufacturers-and-health/647913/

Ransomware via Third Party Exploits

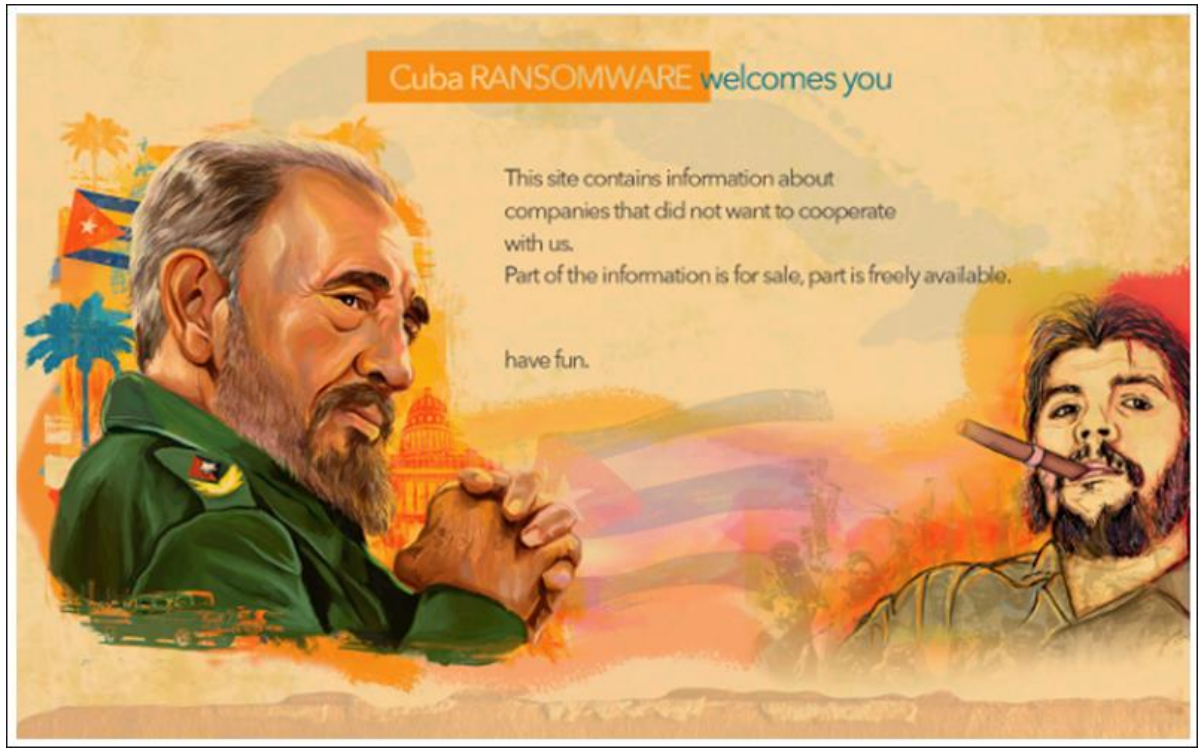


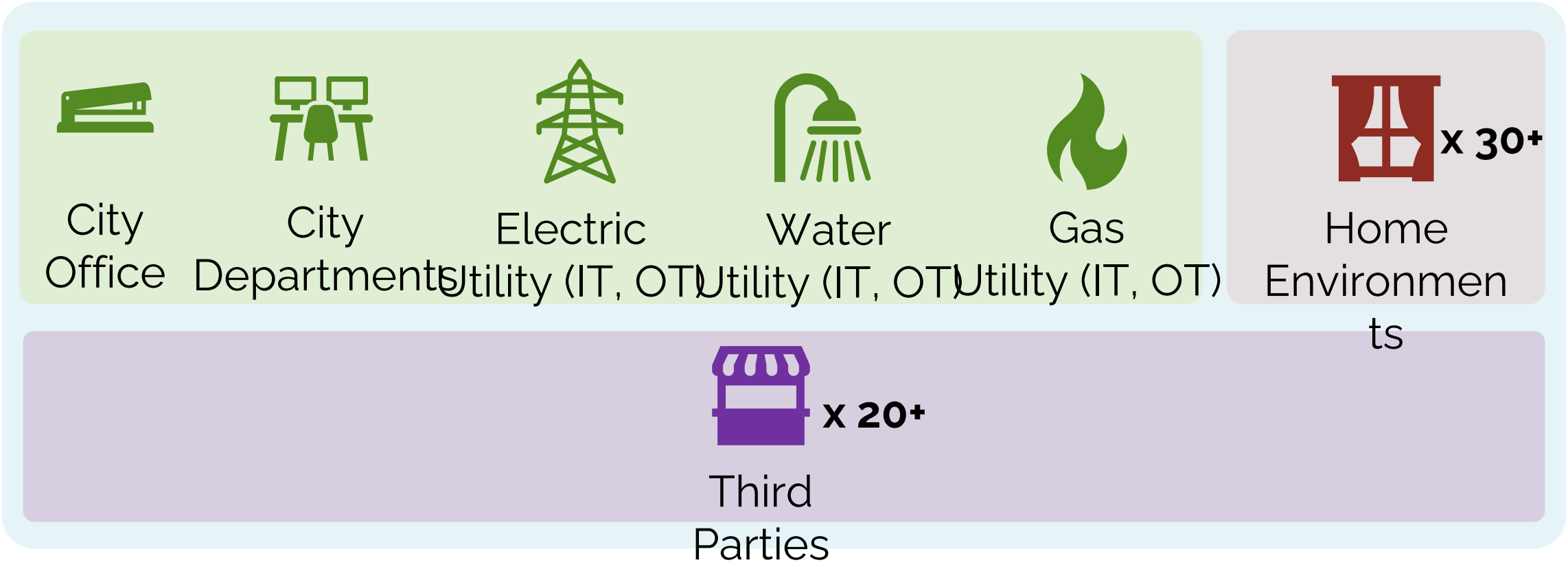
Figure 1: Cuba Ransomware leak site

"A critical infrastructure organization in the U.S. was attacked by the Cuba RANSOMWARE group via a months-old vulnerability in Veeam".

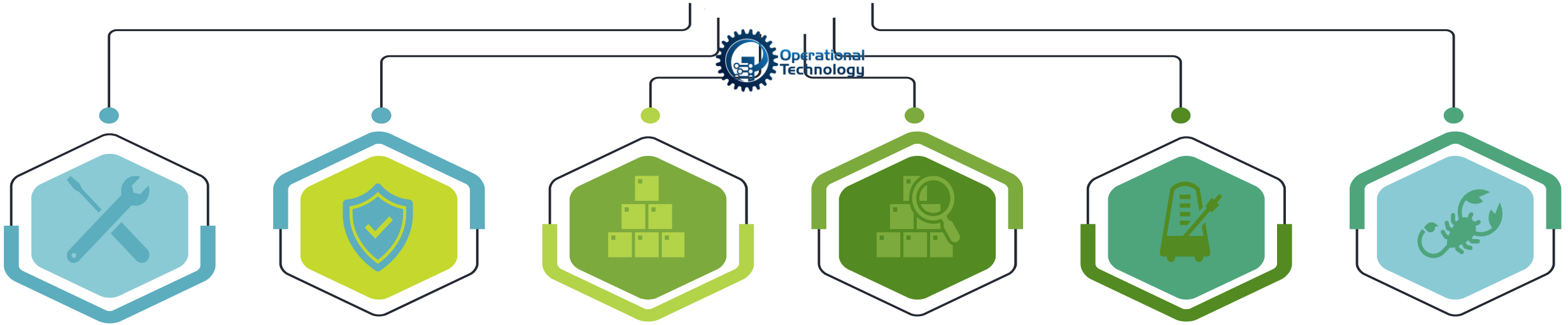
"The vulnerability, which affects Veeam Backup & Replication software, allows an attacker to potentially access credentials stored in the configuration file on victim devices."

Source: https://www.cybersecuritydive.com/news/veeam-exploit-critical-infrastructure/691390/

Distribution Utility Attack Surface



Operational Technology Implications



Utilities typically rely very heavily on their OT vendors for configuration, support, and maintenance

OT vendors vary greatly in their cyber security maturity and capabilities

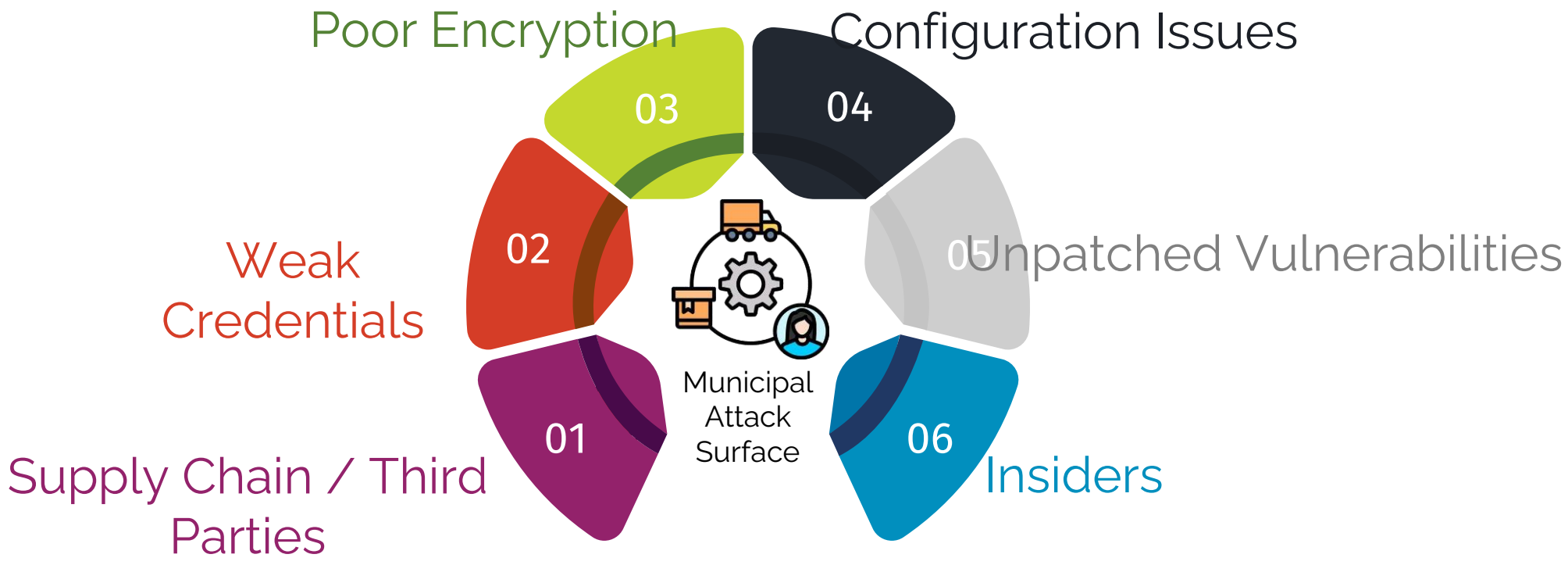
Many installed base vendors are not able to address cyber security adequately

OT malware and cyber security event detection can be difficult

OT patch intervals are typically much longer than IT intervals

OT systems are now an attractive target for threat actors

Attack Vectors



Software Supply Chain Risks

Approximately 18,000 companies were impacted by the compromised SolarWinds Orion Update (1)

Moody's Cyber Risk Outlook Report: "cyberattacks on the software supply chain are raising the threat of damaging reputational trust" (2)

"Critical SAP vulnerabilities spur CISA, researcher pleas for urgent patching. The vulnerabilities could result in a range of attacks, including sensitive data theft, financial fraud, ransomware, disruption of mission critical functions or even operations shutdown." (3)

My perspective: supply chain / third parties now represent a greater cyber risk than insiders

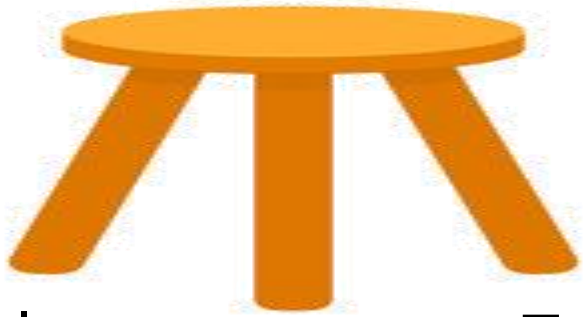
(1) https://www.cybersecuritydive.com/news/cisa-initial-access-vectors-solarwinds-orion
(2) https://www.cybersecuritydive.com/news/supply-chain-attacks-could-open-up-vendor-competition-moodys-says

(3) https://www.cybersecuritydive.com/news/sap-vulnerabilities-urgent-patching

How to Address the Cyber Security Threat Landscape

Cyber Security is a Risk Management Issue

- Cyber Security is not an IT issue, it is a Risk Management issue
- It is not a “one and done”, it is a journey
- Your aim is to increase your cyber maturity over time
- A balanced approach across the “three legs of the cyber stool” is required



People Process Technology

Fundamental Steps for Good “Cyber Hygiene”

1) Engage a cross functional team
2) Adopt standards
3) Balance across the three legs of the stool
4) Deliver awareness training & vigilance
5) Prepare and test Respond and Recovery Plans
6) Manage Key Third Parties

Thank You

Doug Westlund, P.Eng., MBA

Senior VP, Principal Consultant, **Acumen**

dougw@aesi-inc.com

416.997.8833

Secure Generative AI

Florida
GAS UTILITY

FGU Annual Conference

October 11, 2023

Tom Patterson
Managing Director,
Emerging Technology Security
Co-Founder, GenAI Security group
Tom.Patterson@Accenture.com

Secure Generative AI

Florida
GAS UTILITY

FGU Annual Conference

October 11, 2023

Tom Patterson
Managing Director,
Emerging Technology Security
Co-Founder, GenAI Security group
Tom.Patterson@Accenture.com

Managing Director – Emerging Technology Security

Tom Patterson | Accenture | Tom.Patterson@accenture.com

BACKGROUND

Tom is the Managing Director for Emerging Technology Security at **Accenture**, where he serves as the global lead for **quantum** security and **space** security, as well as a leading contributor to **GenAI** security. Tom joined the leadership team to continue his mission to secure the world's **critical infrastructure**, leveraging his background in **national security** policy, emerging technologies, and cyber security expert to provide perspective to both defend and prosper with the emerging technologies used to compute, communicate, and decision.

EXPERIENCE

Accenture Global Quantum Security Lead
Leads development and operations of global quantum security group, including quantum vendor database, post-quantum testbed, and quantum security strategy. Works with strategy, crypto discovery, crypto agility, and QKD products and services.

Accenture Global Space Security Lead
Leads global efforts in space security, focused on providing managed security services in low earth orbit (LEO), as well as entire CIS-Lunar space. Working through build, launch, and operate phases of space security lifecycle. Using key technologies that secure existing satellites, new builds, the International Space Station (ISS), and future lunar surface missions. Responsible for planned launch of Accenture CARET security satellite.

Founding Contributor, Global GenAI Security Practice
Principal author of Trusted GenAI report, that defines the emerging generative artificial intelligence space, provides threat and remediation analysis, and directional frameworks for trusted success with LLMs.

Industry and Academic Activities (Current)
Serving as a Senior Fellow at **Auburn** University's Center for Homeland Security. Serving for more than ten years as **SIFMA'**s Emerging Technology Security executive briefer at annual Security Industries Institute at **Wharton** School. Serve on **FBI'**s Domestic Security Alliance Council (DSAC) as a board advisor.

Post-Quantum Security National Policy (2015-2022)
Served as the President's co-lead for the **White House**'s National Cyber Moonshot report to make the Internet safe by 2030, focused on quantum, 5g, and AI security.

SKILLS and CERTIFICATIONS

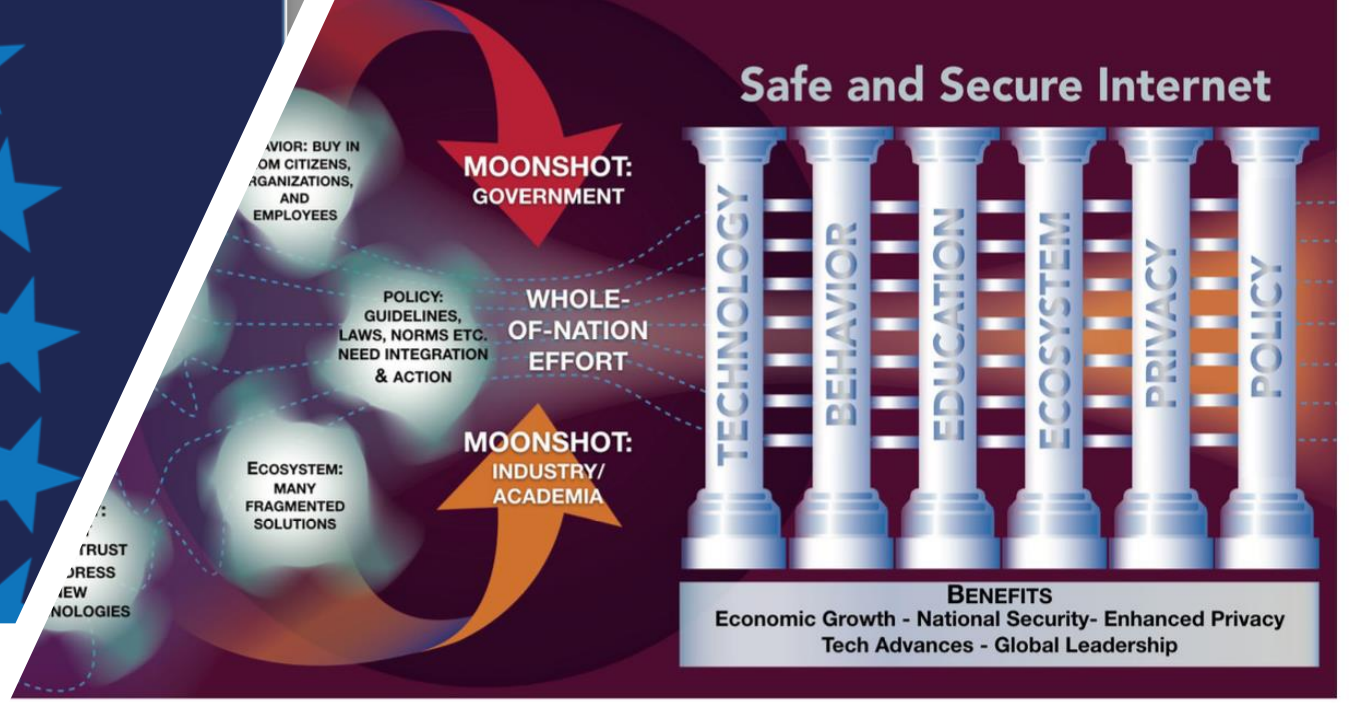
- Post-Quantum Security
- Crypto Agility
- AI/ML Security
- 5/6/g Communications
- Space Security
- OT / SCADA
- Trust
- Resilience

INDUSTRIES

- Financial
- Energy
- Communications
- Manufacturing
- Technology
- Transportation
- Healthcare
- National Security
- Five Eyes

National Cybersecurity Strategy

MARCH 2023



igure 2: *The NSTAC's recommendation for the Cybersecurity Moonshot Initiative's Strategic Pillars—a proposed organizational construct for the broad but interdependent categories of activities required.*

NATIONAL SECURITY TELECOMMUNICATIONS ADVISORY COMMITTEE

NSTAC

NSTAC Report to the Pres

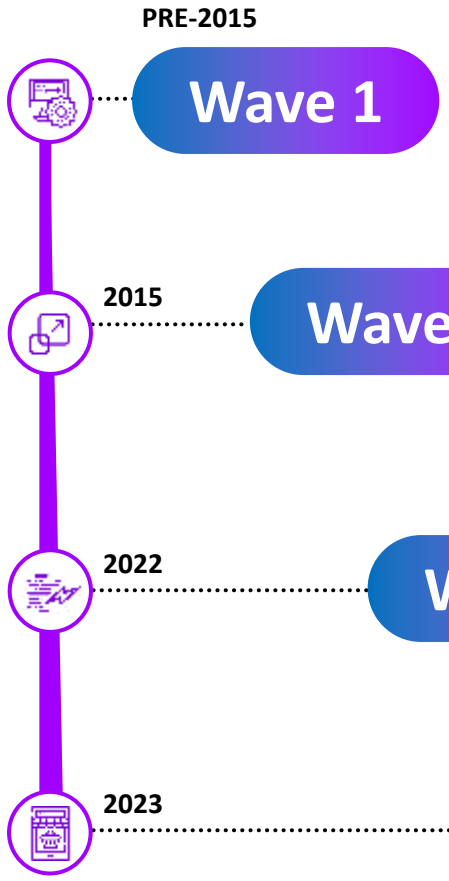
…yption is foundational to cybersecurity and global commerce. It is the primary way we …r data online, validate end users, authenticate signatures, and certify the accuracy of …ion. But quantum computing has the potential to break some of the most ubiquitous …tion standards deployed today. We must prioritize and accelerate investments in widespread …cement of hardware, software, and services that can be easily compromised by quantum …puters so that information is protected against future attacks.

…o balance the promotion and advancement of quantum computing against threats posed to digital systems, NSM 10, "Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems," establishes a process for the timely transition of the country's cryptographic systems to interoperable quantum-resistant cryptography. The Federal

The future happens gradually – and then all at once.

Generative AI is a step change in the evolution of AI

More data, more compute, new outcomes, more risk



Small models reign supreme (Pre-2015)
5+ years ago, small models were considered “state of the art.” They excelled at analytical tasks and enabled time prediction to fraud classification.

The race to scale (2015-Today)
Two landmark moments occurred. Google introduced the concept of transformers in NLP. Stanford aptly classified these large language models (LLMs) as foundation models. Trained on broad data at scale and adaptable to a wide range of downstream tasks, LLMs mimicked human performance in speech, vision, language understanding, and comprehension.

Better, faster, cheaper (2022+)
Compute gets cheaper, and algorithms and large models become better. New techniques, like diffusion models, shrink the costs required to train and run inference.

Killer apps emerge (Now)
With the platform layer solidifying, foundation models continue to become better/ faster/ cheaper. Just as mobile fostered an app marketplace, we expect killer apps to emerge for Generative AI.

Every utility needs a holistic set of AI capabilities

Diagnostic

Why did this happen?
Analyze
Scenario
Segment

Predictive

What might happen in the future?	What should we do next?
Pattern	Simulate
Forecast	Optimize
Model	Recommend

Generative

How AI can help with the execution?
Advise
Create
Code
Automate
Protect

Risks associated with utilization of Generative AI

Consideration of associated risks is an important piece in the decision to adopt Generative AI

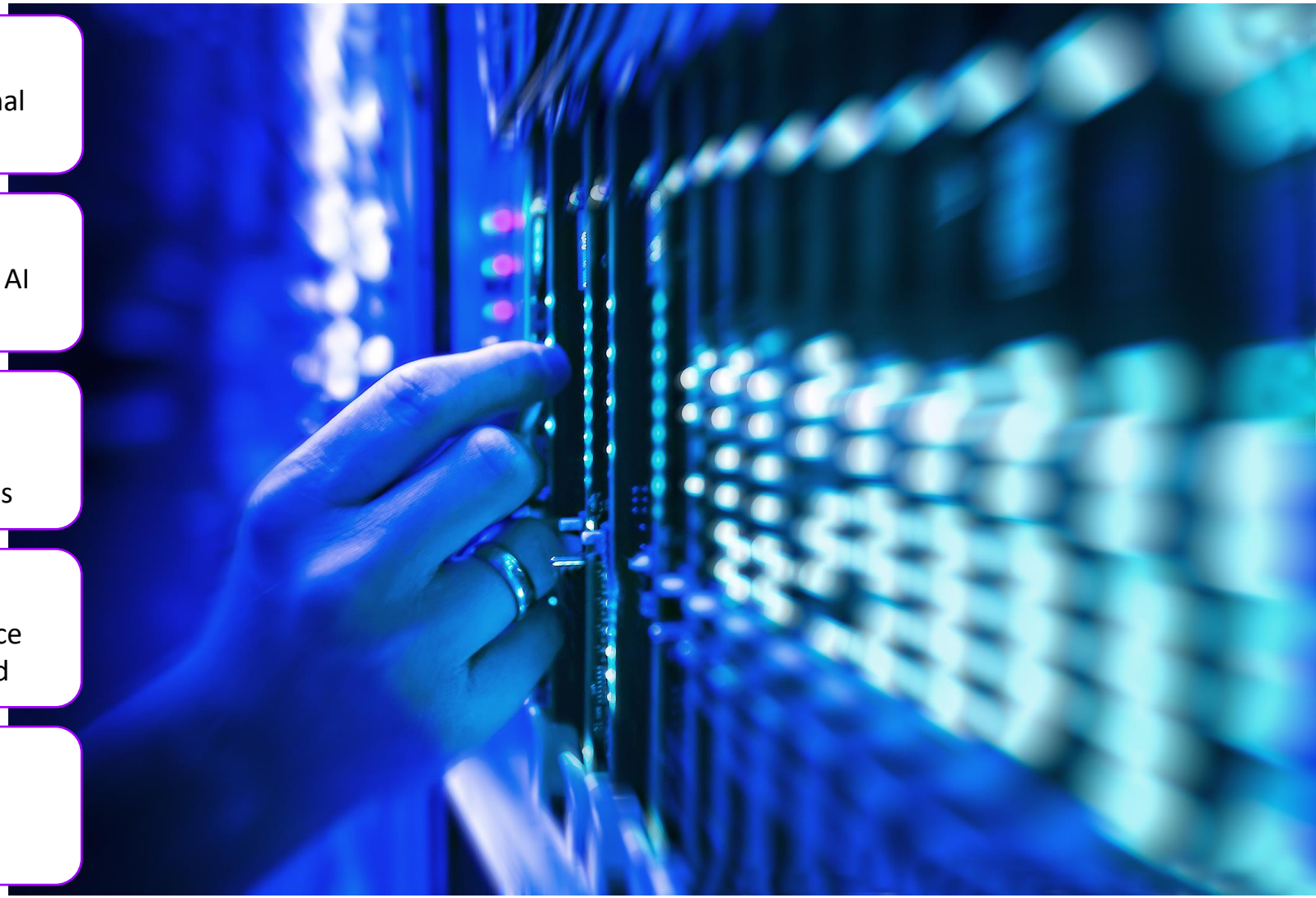
Sensitive Data Exposure
Gen AI models trained on sensitive data creates additional risk of exposure of sensitive information

Gen AI Model Disruption
Attacks on AI infrastructure expose risks to disruption of AI models and dependent business operations

Gen AI Bias
Unconscious biases in training data can lead to unfair outcomes, resulting in reputational and legal implications

GenAI Attack Vectors
Worm.AI, Call Center deceptions, Identity Theft, and voice and video phishing are all easily enabled and popularized

Data Manipulation
Manipulation of training data can lead to distorted AI results, outcome biases, and damaged business insights

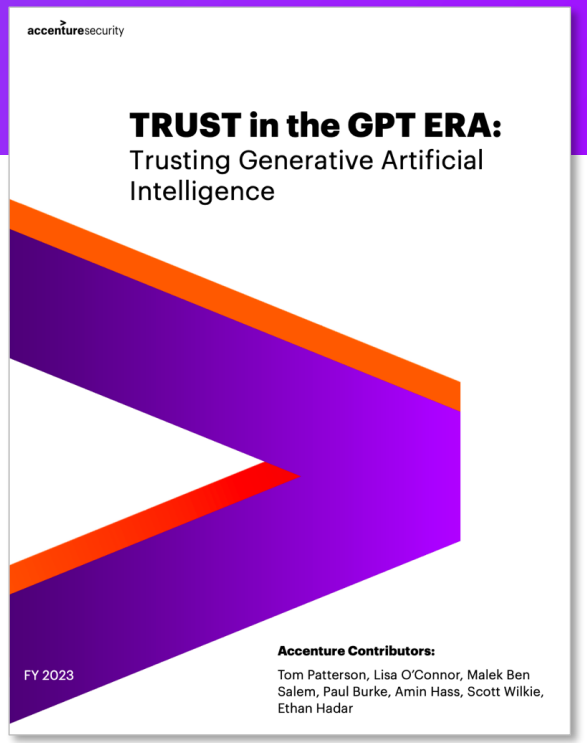


What is “Trustworthy” Generative AI?

*“To be **trustworthy, AI** technologies must appropriately reflect characteristics such **as** […] **privacy, reliability, robustness, safety and security or resilience** to attacks*

*….Developing and using AI in ways that are **ethical, reduce bias, promote fairness and protect privacy** is **essential for fostering a positive effect on society**…”*

–White House on Trusted AI, 2023

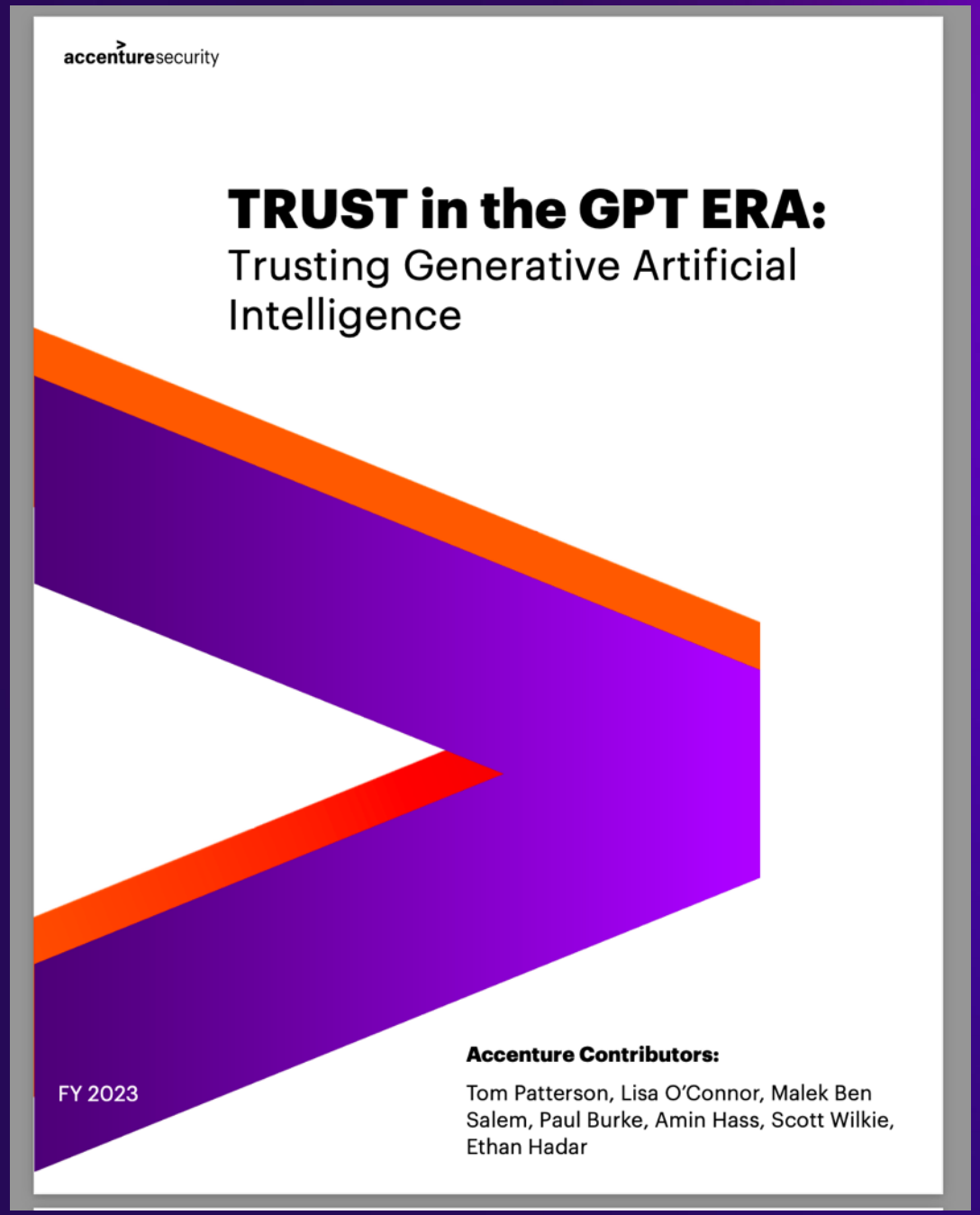


Generative AI projects and products are at **heightened risk of compromise without well planned and executed security strategy at the start**. Decision on **training data, controls to manage biases, policies and training are critical**. Managing **unexpected exfiltration of data** is vital, and providing **transparency of the entire generative AI process** is required to maximize user acceptance.

There are new models, frameworks and technologies available that help guide **AI programs forward with trust, security and privacy** throughout. Focusing on **trustworthy AI strategies, trust by design, trusted AI collaboration** and continuous monitoring help build and operate successful systems.

Value for Enterprises

→ **Greater acceptance of results**
→ **Lower risk of compromise**
→ **Easier regulatory compliance**



Contents

- Overview....3
- ChatGPT Wakes up the World to the Power of Generative AI....3
- What is GPT Today?....4
- Opportunity of Generative AI for Good....5
- Risks of GPT for Bad....7
- Key Trust Areas to Understand with GPT....8
- Key Considerations/Recommendations in the GPT Era....9
- What's Ahead in GPT....10
- Accenture INTERNAL Trusted GPT Point of View....11
- Accenture Resources:....14

With the arrival of Gen AI, we are at an inflection point

98%

of global executives agree AI foundation models will play an important role in organizations' strategies in the next 3 to 5 years

40%

of all working hours can be impacted by LLMs like GPT-4

We need to act now to adopt AI, or **risk falling behind**

But if we don't build on a **foundation of trust**,

we face increased risk of **compromise, non-compliance,** and **reputational damage**

Source: AI for Everyone, Accenture, March 2023

Five Critical Cybersecurity Areas that Enable GenAI

Access to, and investment in, cybersecurity here will accelerate sustainable value creation

01 Compute

The more complex and useful AI techniques require compute processing power to **train, run and act**.

Utilizing advanced compute power at lower costs.

02 Data

AI requires data to train, learn and act. The **more information** is **readily available**, **accessible** and **accurate** will increase the successes from AI.

Unleash the value **from Dark Data**—information that is currently stored without insights.

03 Ecosystem

Investments in digital capabilities, including **Internet of Things** and Platforms, expands the amount and type of information available to AI solutions.

The use of sensors, implemented in physical environments beyond computers and mobile phones.

04 Experience

AI enables technology designed specifically for **individual human behavior** and **interactions.**

How well the customer's goals and objectives are known across their lifecycle will enhance not only the quality of the experience, but the effectiveness of the product or service.

05 Talent

Need to have the resource talent to **design**, **craft** and **manage** the AI solutions.

Empower employee to **learn** how to best leverage the AI augmentation capabilities.

Governance **Security** **Resilience** **Innovation**

Thank you

Florida GAS UTILITY

Tom Patterson

Accenture Managing Director,
Emerging Technology Security

Global Lead, Quantum Security
Global Lead, Space Security
Co-Founder, GenAI Security

Tom.Patterson@Accenture.com