September 21, 2021

Rehumanizing Work
ALLIANCE SUMMIT 2021

Cyber Security. Your biggest business risk & liability is one click away.

Jerry Leishman (EVP/National Security & Compliance Director)
Jerry.leishman@cortacgroup.com

Robert King (Chief Information Security Officer)
Robert.king@fswb.com

CORTAC GROUP

1st SouthWest Bank

Agenda

National View of Cybersecurity

Today’s Financial Industry Regulation

Your Path Forward

Insights and Best Practices

Q&A

Compliant. Secure. Risk Optimized.

NATIONAL SECURITY & DEFENSE LANDSCAPE

DEFENSE & AEROSPACE

"The United States' strategic competitors and adversaries are conducting cyber-enabled campaigns to ***erode U.S. military advantages, threaten our infrastructure, and reduce our economic prosperity.***

This constitutes one of our most critical national security concerns."

Department of Defense

NATIONAL SECURITY & DEFENSE LANDSCAPE

HAPPENING TODAY

Lockheed Martin, General Dynamics, Boeing, Tesla, and SpaceX are among dozens of companies named as victims of compromised data, accessed through the hacking of precision parts manufacturer **Visser Precision LLC**, a Denver Colorado-based aerospace, automotive and industrial parts manufacturer.

Other Recent National Events

Solar Winds - IT
Colonial Pipeline – Oil & Gas
JBS Meats – Consumer Meat
McDonalds - Consumer

DoD – Cybersecurity Maturity Model Certification (CMMC)
Biden Executive Order – Federal
Dept Homeland Security – New Security Requirements for Oil & Gas
Biden Whitehouse Order – Critical Infrastructure

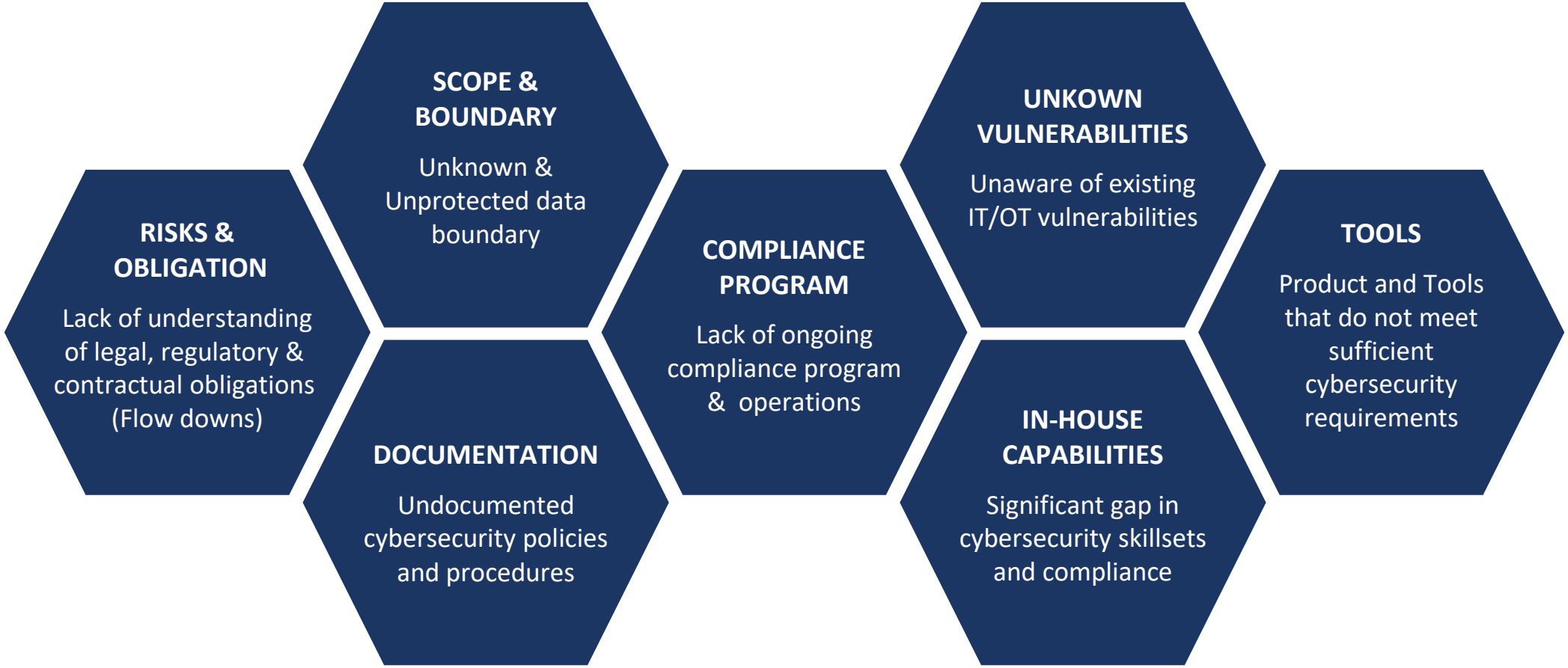
WHY IS THIS HAPPENING?

- Commercial and Defense Industrial Base (DIBs) have lived safely on the home front
- Economic warfare is the new model. Adversaries see suppliers' intellectual property as treasure to hold ransom.
- Customer IP is a valuable asset and companies will pay ransom to get their information back.
- Colonial Pipeline, JBS, McDonalds and others are experiencing supply chain disruption affecting American's day to day lives

- The IP is digital, which has made cyberspace into a battlefield. This makes commercial and government suppliers into combatants.
- The US's treasure is being lost and this is getting worse. See the SolarWinds hack. As Understanding of Russian Hacking Grows, So Does Alarm - The New York Times (nytimes.com)
- The DoD says we need to fix this and is asking suppliers if they're on board. Biden says we need to protect military, economic & public safety of USA.

YOU'RE NOT ALONE

COMMON DATA PROTECTION GAPS



YOUR OPTIONS

Yes, this is going to cost money.

You have four options:

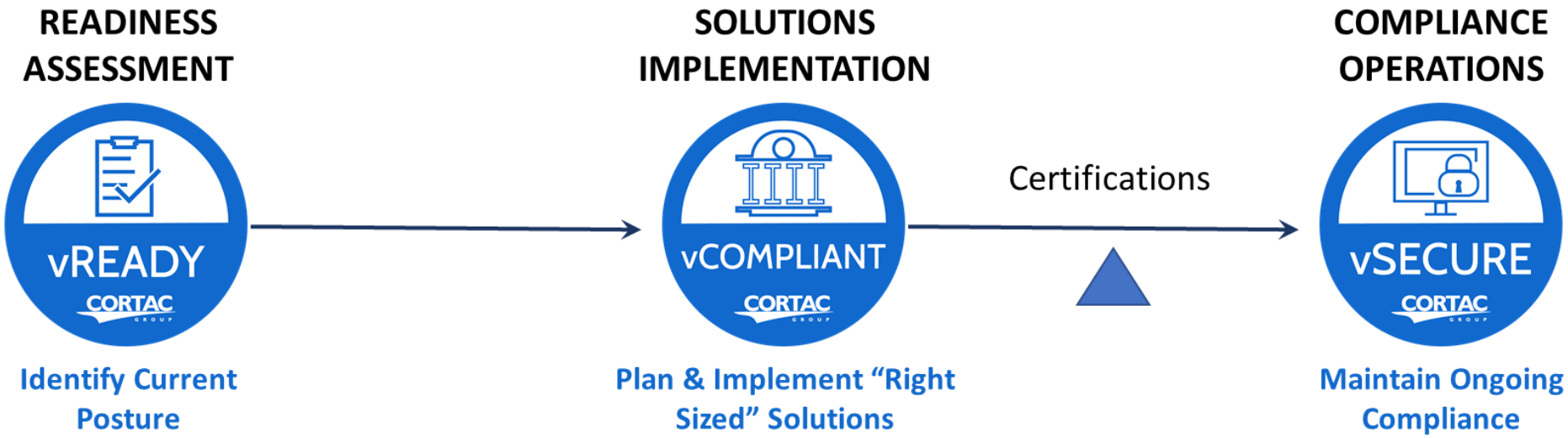
1. Proactively secure your data and your business.
2. Implement a minimal solution to protect yours and customer data.
3. Fix security deficiencies, write documentation, and prepare for a commercial and government contracts.
4. Do nothing. Break your contracts. Lose data.

Always Under Attack

TODAYS FINANCIAL INDUSTRY

- 238% increase in attacks in 2020
- Average cost of data breach is +$5m
- Heavily regulated
- Protecting customers from themselves
- Third-Party Vendors

YOUR PATH FORWARD

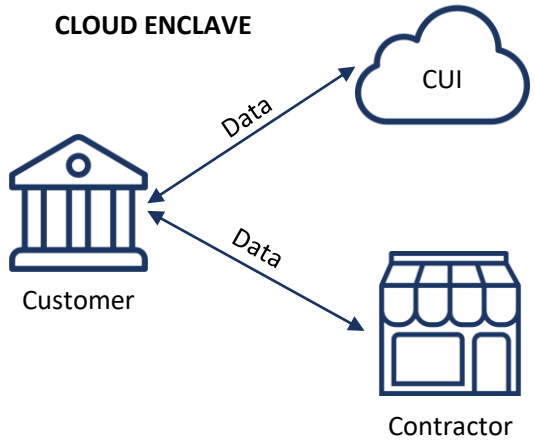


- Improve process and practices to protect information from being disclosed to unauthorized entities and individuals and ensuring ongoing resiliency to future nefarious attacks
- Reduce risk of supply chain exfiltration of corporate and customer intellectual and sensitive property by increasing internal OT/IT system information protection, governance, and security.
- Enforce a systematic compliance program that demonstrates information protection resiliency and enhances reasonable due care and diligence
- Position organization to win more business and competitive advantage and value

COMMON SOLUTION GAPS

DOCUMENTATION

TECHNICAL SOLUTIONS



SECURITY & COMPLIANCE PROGRAM MANAGEMENT

PRACTICAL TAKEAWAYS FOR EVERY SIZE ORGANIZATION

- Train, Test, Train again
- Don’t know them don’t trust them
- Guard against your trusted vendors
- Backup your Backup
- Know how to buy crypto

KEY TAKEAWAYS

- Information Protection is a C-Level Business Risk, Not just an IT issue
  - In-house council & compliance officers are responsible to ensure all regulatory and cybersecurity risk is addressed
- Significant organizational leadership collaboration & alignment will be required
  - Inhouse counsel, compliance officer, CIO, and business product owners own CUI, from Sales to Shipping, and crosses people, process and technology
- Can't fake it till you make it anymore
  - You will have to pay to play to receive DoD contract awards and meet customer contract requirements
- Efficiency and cost optimization will require a systematic enterprise approach
  - instead of whack a mole
- Cybersecurity Insurance rates and pre-qualifications are increasing
  - You won't get coverage or high premium costs based on your security & compliance posture
- Data Protection shortcuts won't get you there anymore
  - Data enclaves and awkward workflows only increase information leakage and exfiltration risk
- You will need experts to help
  - Most organizations do not have the skills and capabilities to understand and implement solutions to meet regulatory requirements, thus leaving the organization at high risk of non-compliance and penalties
- Regulatory, legal and contractual compliance, or similar, will become cost of modern business
  - Federal, State, Local, International and Commercial Contracts will adopt DoD like baseline requirements in their contracts
- Get started now – Security Gaps & Non-Compliance Penalties are high & tide is rising
  - Most organizations have a low maturity and a significant amount of work to do to meet upcoming upcoming compliance requirements and certification to keep existing contracts and win new business

CONTACT INFORMATION

Jerry Leishman

- jerry.leishman@cortacgroup.com
- www.cortacgroup.com

Robert King

- robert.king@fswb.com
- fswb.com

THANK YOU!!

Our Story

INTRODUCTION TO CORTAC

BY THE NUMBERS

13 Years in Business

79 Clients (21 in the Fortune 500)

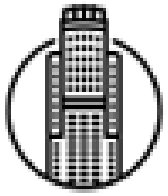
350+ Projects Delivered

30+ Countries Serviced

100+ Team Members

OUR OFFICES

Seattle, WA



Los Angeles, CA

Washington DC

KEY CLIENTS

Microsoft

BAE SYSTEMS

Anthem

LOCKHEED MARTIN

SAP Concur

BLUE ORIGIN

amazon web services

BOEING

SECURITY & COMPLIANCE

Regulatory Compliance (vREADY)

- Regulatory risk & obligation strategies for ITAR, DFARS, CMMC, and FedRAMP
- Readiness and gap assessments & recommendations
- Policy & Practices Development
- Certification package development
- Training

Technical Solutions & Architecture (vCOMPLIANCE)

- Enterprise security architecture strategy and design
- Identification of productivity and infrastructure solutions
- Recommendation of security configurations
- Data Identification, classification and workflow management recommendations
- System integration planning (e.g., M&A)

Compliance Program Execution (vSECURE)

- Compliance Program Management
- Microsoft/Other partner ecosystem product & solutions
- Project & Program implementation execution and delivery
- Compliance analytics and reporting
- Supply chain risk assessment, management & reporting
- Insider Threat

Cybersecurity Due Care

- Pre-breach cybersecurity due care assessment
- Post-breach cybersecurity due care assessment
- 3rd party contractor performance audit failure due care (ITAR/EAR/DFARS/CMMC)
- M&A security & compliance risk assessments

READINESS ASSESSMENT (vREADY)

CORTAC GROUP
Readiness Assessment

Independent and Experienced Perspective

- Understand Risks & Obligations - Inspect, review, and verify the applicable legal, regulatory, and contractual requirements and associated risks and obligations
- Understand Data Boundary - Identify & document sensitive information data flows and boundaries for ITAR, EAR, FCI and CUI data
- Identify Baseline Security & Compliance Gaps & Recommendations - Identity gaps and receive actionable mitigation recommendations and solutions

vReady Report Includes

- Baseline Assessment - Detailed “current state” assessment report based on framework such as NIST 800-171 and/or CMMC Level 3
- DoD Reporting– Establish Supplier Performance Risk System (SPRS) score to meet interim DFARS rule as of November 30, 2020
- Roadmap - Executive roadmap based on risk to guide cybersecurity investment decisions and future planning activities

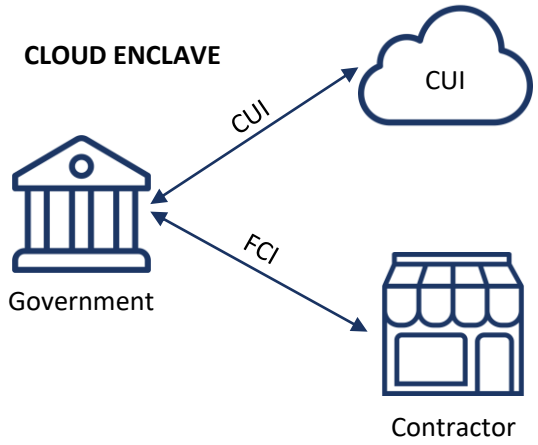
Right Sized & Cost Optimized Solutions

SOLUTION AREAS (vCOMPLIANT)

DOCUMENTATION

Documentation requires a foundational set of policies, procedures, and documentation required to demonstrate due care and meet NIST 800-171 & CMMC assessment criteria. Initial documentation is inventoried and assessed for completeness and reviewed for applicability and institutionalization within the organization. All documentation gaps will be filled and updated to "audit ready" state based for targeted solution architecture.

TECHNICAL SOLUTIONS



NIST 800-171 & CMMC L3 cloud solutions are ideal for small to medium sized organizations that can isolate their FCI and CUI from infrastructure, applications and vendors without significant interruption to user processes and experience. It consists of a standardized environment with limited functionality that can only be accessed via virtual desktops with constrained configurations.

SECURITY & COMPLIANCE PROGRAM MANAGEMENT

Compliance Program (vSECURE) is a NIST 800-171 and CMMC standardized security & compliance program service that enables organizations to secure their data and achieve CMMC Level 3 "audit ready" and maintain ongoing resiliency requirements. The heavy lifting is outsourced, leaving only critical decisions to customers.

MANAGED COMPLIANCE OPERATIONS (vSECURE)

Business Alignment: Ensures all functions across the organization are driving toward the same goals and quality standards in support of the business.

Security & Compliance: The supervision required to ensure an environment is adequately secure while complying with standards.

Technology Architecture & Operations: The design, configuration, and monitoring to ensure an environment works as intended by Security & Compliance and Business Operations in support of business needs.

Business Operations: Support required to fund and administer the environment.

Enterprise: Corporate-level support for enterprise security.

WHY CORTAC GROUP?

BROAD & DEEP EXPERIENCE

- Former Fortune 100 & Government Executives with leadership across governance, risk, and IT compliance disciplines to guide your teams
- Broad and deep knowledge of U.S. and International government regulations and standards across industries and geographic regions
- Experience delivering compliance, engineering, and operations solutions to defense, aerospace, manufacturing, healthcare, and technology organizations including Boeing, Samuel & Son, Microsoft, Cargill, & Snohomish County PUD

SUBJECT MATTER EXPERTISE

Security, Privacy, and Compliance

- Extensive compliance and engineering experience helping organizations navigate U.S. regulatory requirements including Cybersecurity Maturity Model Certification (CMMC), Federal Information Security Management Act (FISMA), FedRAMP Provisional Authority to Operate (PATO), Defense Information Security Agency (DISA), ITAR, DFARS, Import/Export controls, CJIS, and IRS 1075
- Significant engineering experience developing compliant IT solutions through the full lifecycle including requirements, architecture, design, implementation and operations
- Cyber security thought leadership working with external standards bodies and Federal Cyber organizations to enhance industry security best practices across a broad spectrum of standards including U.S. Federal, SOC, ISSO 27001/2, U.K G Cloud and Austrian Federal iRAP
- Consultant certifications include CISSP, CISP, CIPP, IAPP, CSM, & PMI

DIFFERENTIATED VALUE PROPOSITION

- Full set of GRC advisory services: strategy, assessment, remediation, documentation, compliance program management, and audit prep
- Highly collaborative and agile approach, optimized for rapid delivery and value
- Experienced consultants, extensive network, and low employee turnover
- Consistently high-quality deliverables & resources. “Quality Always”
- Microsoft preferred partner for large, complex, Defense & Aerospace customers