CyberTech Solutions –
Information Technology (IT) vs. Operational Technology (OT)

Daniel Sliverman
Greg Chevalier
Brian Retherford
June 27, 2023

The Hartford at a Glance

Financial Highlights (as of 12/2022)[2]

2022 Revenues: $22.4B
2022 Shareholder equity: $13.6B
Treasury Listing: $3.0B
Hartford Fire Insurance Company (A+/A1/A+)
A.M. Best/Moody's/Standard & Poor's

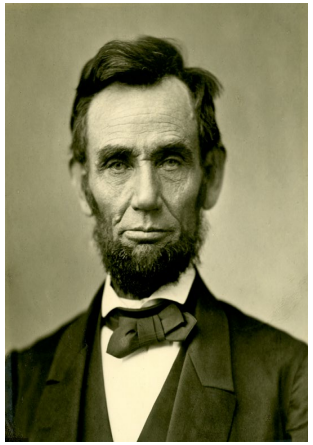
US Market Rankings*

No. 2 Professional Liability insurer[3]
No. 3 Cyber Liability insurer[4]
No. 2 Workers' Compensation insurer
No. 160 on Fortune 500 List[5]
Top 10 in Insurance P&C category on Fortune 500 List

4.8 OUT OF 5 STARS FOR CLAIM EXPERIENCE[1]

200 YEARS
EXPERIENCE INSURING BUSINESS

2023 WORLD'S MOST ETHICAL COMPANIES® ETHISPHERE 14-TIME HONOREE



Founded in 1810 with over approximately 18,100 employees to date, The Hartford has over 200 years of expertise and is a leader in property casualty insurance, group benefits and mutual funds.

1 Customer surveys have been collected and tabulated by The Hartford and reviews are not representative of all customers.
2 https://ir.thehartford.com/financial-ratings/financial-strength/default.aspx
3 https://advisorsmith.com/professional-liability-insurance/best-professional-liability-insurance-companies/
4 https://www.insurancebusinessmag.com/us/news/cyber/top-10-cyber-insurance-providers-in-the-us-in-2022-326912.aspx
5 https://fortune.com/ranking/fortune500/2022/search/Fortune 500 | Fortune
World's Most Ethical Companies" and "Ethisphere" names and marks are registered trademarks of Ethisphere LLC.

Cyber Coverage Overview

Cyber Liability

- Defense and damages:
  - Data breach and privacy lawsuits
  - Network interruption lawsuits
- Fines and penalties
  - Data breach fines and proceedings, PCI fines and assessments
- Data breach response expense
  - Breach coach, forensic investigation, notification, credit monitoring, PR consultant

Cyber First Party

- Incident response
  - Forensic investigation, recovery assistance
- Data restoration
- Business interruption loss
  - Net income loss, extra expense
- Extortion negotiation and payment
- Electronic theft of money and securities

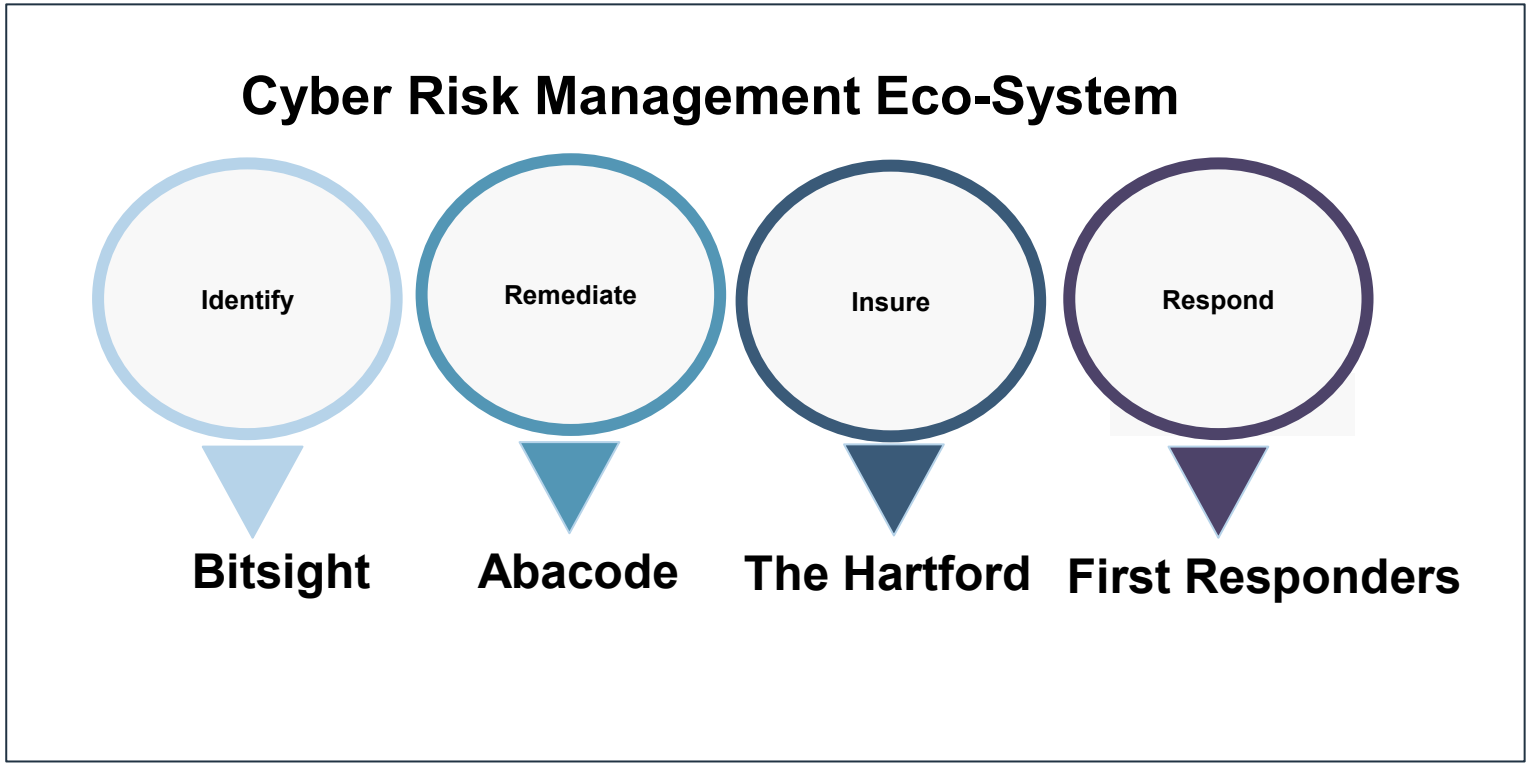
Cyber Coverage at The Hartford*

The Hartford provides cyber coverage to more than 580,000 policyholders through stand-alone cyber, technology errors and omissions, management liability and endorsements to general liability and property.

	Cyber Liability	Cyber 1st Party
CyberChoice First Response	✓	✓
CyberChoice Secure	✓	✓
CyberChoice Professional	✓	✓
FailSafe	✓	✓
FailSafe (Spectrum Endorsement)	✓	
Private Choice Premier	✓	✓
Life Sciences Elite	✓	
General Liability Choice	✓	
Spectrum Data Breach	✓	✓
Spectrum First Party Cyber		✓
Y-Risk	✓	✓

**The Hartford cyber products may not include all coverage components displayed in the coverage description under Cyber Liability and Cyber First Party*

Cyber Underwriting and Risk Mitigation



https://www.bitsight.com/ https://www.abacode.com/

Greg Chevalier
Senior Vice President – Abacode, Inc.
greg.chevalier@abacode.com
678-612-7652

- ✓ 18 Years Senior Advisor to growth Cybersecurity Companies
- ✓ 12 Years IBM
- ✓ 6 Years startups through exit (IPO and Acquisition)

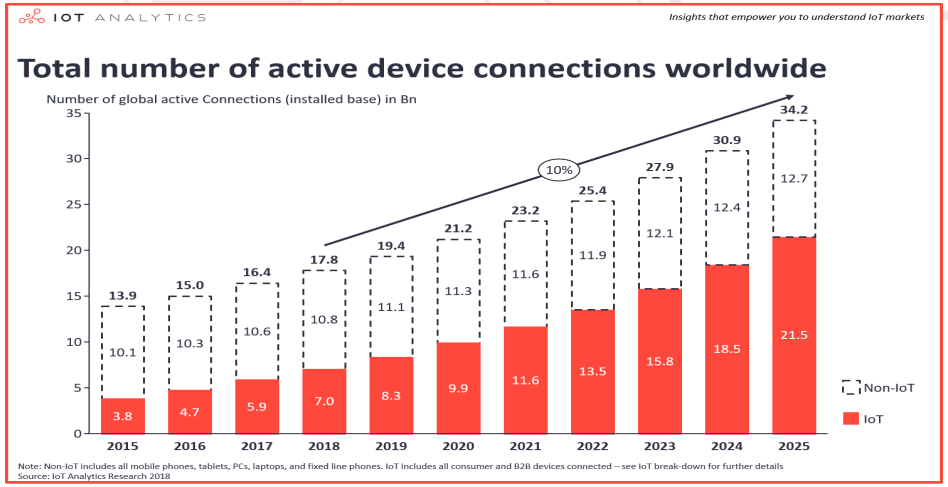
Brian Retherford
Vice President, Cyber Technology & Services – RMC Global

bretherford@rmcglobal.com
816.665.5304

- ✓ 15+ years US Army (Cyber Command)
- ✓ McKinsey & Company (Cyber & Risk Practice)
- ✓ 10+ years in cybersecurity – Federal and private sector

How Did We Get Here?

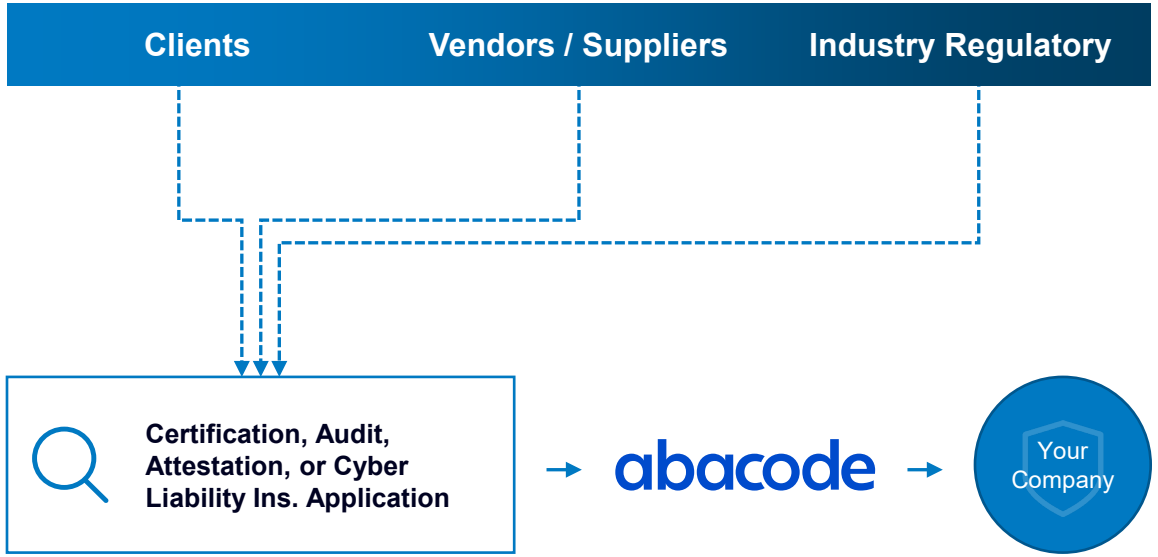
- What percent of the global data was created in the last 2 years?
  - 90%
- What is the increase in internet connected devices in the last 2 years?
  - IT = 11.3 Billion to 12.1 Billion
  - IoT = 9.9 Billion to 15.8 Billion
  - Data is accessible from anything anywhere!
- Initial event that drove DoD to the CMMC Initiative? (appendix conversation)
  - NETWORKS / CYBER, PENTAGON: CMMC was initiated to stop Cyber Espionage Like Chinese Theft of F-35 Data
  - China's J-31 stealth fighter is built in part on plans taken from the US as part of a long-running espionage program. The breach occurred in 2007, and came through a subcontractor to Lockheed Martin, the principal maker of the F-35.
- Percent of data breaches as a result of human error?
  - 95%



BREAKING DEFENSE

The Eco System Of Cybersecurity & Compliance

Prospects and Clients expect a level of data protection.



Business Drivers

- Condition of doing business (clients / supply chain / industry)
- All things CMMC – key message: **The Primes are pushing this down** as a strong requirement!!!
- Cyber Insurance (new / renewal)
- Capital infusion events – Private Equity / Other
- Merger & Acquisition risk reduction

Compliance and impact on revenue:

- ✓ It's about you
  - ➢ Your choice – positive or negative impact on revenue
- ✓ It's about your suppliers
  - ➢ Are they a risk to your business
- ✓ It's about your clients
  - ➢ They are asking you for this
  - ➢ Creates competitive advantage
- ✓ It is a condition of doing business
  - ➢ Contracts
  - ➢ Financial / capital infusion considerations

Why Are We Interested In OT?

Technology Security Market Overview

15.5 USD BILLION 2022

32.4 USD BILLION 2027

CAGR of 15.8%

The global OT security market is expected to be worth USD 32.4 billion by 2027, growing at CAGR of 15.8% during the forecast period.

The Americas is estimated to hold the largest market share of the global OT security market in 2022 and Asia Pacific is projected to grow at the highest CAGR during the forecast period.

The market growth can be attributed to the increased use of digital technologies in industrial systems and convergence of IT and OT systems to fuel the growth of OT security.

Countries are showing huge opportunities for the OT solutions due to the presence of the maximum number of OT vendors in the market and strict government regulations because of the increment of cyberattacks on the OT systems.

Terminology

- IT Security – Information Technology
  - Servers, routers, switches, firewalls, end points (desktop / laptop)
- OT Security – Operational Technology
  - **Manufacturing:** Robots, controllers, manufacturing equipment, etc. (Think Chrysler, Ford, **Hospital system** heart monitoring systems)
- IoT – Internet of things:
    - Smart home devices, smart cars, smart cities, etc…..
- Abacode Emphasis is IT Security, and OT Security

Why is this conversation relevant to every business?

abacode

Examples of OT impacting every business, not limited to manufacturers & utilities, can include:

- Building management systems
- Fire control systems, and
- Physical access control mechanisms
- Anything your business relies upon that includes an IoT device

Tech companies and other vendors serving Manufacturers, Utilities, Industrial operators and the like:

- Have a security liability exposure to passing vulnerabilities to these types of clients:
  - Companies delivering software risk spreading malware via open source, remote patching
  - Vendors connecting remotely to their clients such as MSP's may pass malware to their clients, a conduit exposure

THE HARTFORD

We Need To Pay Attention

- Older systems have “lack of intelligence”
- Still connected to networks that connect back to corporate
  - Inability to effectively monitor
- Vendors have publicly stated they are out of date
  - Allows hackers to clearly identify the most vulnerable OT Systems

TECHNOLOGY 〉 CYBERSECURITY | June 21, 2022

Operational technology riddled with security vulnerabilities, new research finds

Study finds 56 vulnerabilities in popular OT devices, many of which would allow remote code execution.

In The News

Ransomware attack temporarily shuts down Dole production, disrupts food supplies

FEB 23, 2023

- Effects of cyberattacks on OT environments
  - Of 64 OT cyberattacks publicly reported in 2021 (an increase of 140 percent over the number reported in 2020), approximately 35 percent had physical consequences, and the estimated damages were **$140 million per incident**

- Industrial cybersecurity company Dragos today disclosed what it describes as a "cybersecurity event"
  - "On May 8, 2023, a known cybercriminal group attempted and failed at an extortion scheme against Dragos. No Dragos systems were breached, including anything related to the Dragos Platform," the company

The Business Equation

- I bet, with precision; you can immediately measure the impact on manufacturing downtime
  - You know your immediate impact to revenue and immediate impact to client satisfaction

- With IT outage, probably not so much…..
  - Major inconvenience, business will run slow
  - You have a good estimate on the financial impact / cost to recover
  - But, in a lot of cases you can still manufacture products

- Well guess who else also knows this? The BAD ACTORS
  - Bad actors have realized significant vulnerabilities in OT
  - Most all OT vendors publicly publish the vulnerabilities – roadmap to a hack
  - This is where the money is
  - Ransoms have increased 4 fold ++

Abacode Approach To OT

- Evaluated what is “transferable”
- Managed Cybersecurity & Compliance Provider
- Operate Two - 24 / 7 / 365 Security Operations Center (IT/OT)
- Full time eyes on glass
- Assessments and frameworks transferred to strategic partner

- Abacode Strategic Partner
- Global OT and Critical Infrastructure Consultancy
- Highly scalable feet on the street – global
- Full range of disciplines in all things OT
- Executing projects today around the Globe with WestRock-level complexity

The Handoff and Integration

Inventory → Controls Assessment → OT Pen Testing → Remediation Plan and architecture → OT Monitoring → On going Continuous Assessment

RMC ASSURING TOMORROW

RMC ASSURING TOMORROW

abacode

abacode

RMC ASSURING TOMORROW

On going Continuous Assessment
Often rotating plants for a multi plant client (1 per month over several years)

Brian Retherford
Vice President, Cyber Technology & Services – RMC Global

bretherford@rmcglobal.com
816.665.5304

- ✓ 15+ years US Army (Cyber Command)
- ✓ McKinsey & Company (Cyber & Risk Practice)
- ✓ 10+ years in cybersecurity – Federal and private sector

IT vs. OT – how is it different?

	Information Technology	Operational Technology
Common examples	Personal computers, phones, cloud services	Manufacturing control systems; valve regulators, building control systems
Communicates through	Primarily via TCP/IP	Dozens of propriety protocols (e.g., MODbus, Serial, OpenADR)
Prioritizes…	Data protection and security - Confidentiality, Integrity, Availability	Uptime, safety
Managed…	Centrally; corporate networks can dictate security policy	Distributed; updates/patches are done in the field with often minimal oversight or tracking
Average device lifespan	2-5 years	15-20+ years

Common misconceptions – OT/ICS

- Believing air-gapped systems are completely secure
- Underestimating the sophistication of attackers
- Assuming that compliance equals security

Real-world example

IRAN - The Stuxnet worm demonstrated that air-gapped systems can still be compromised, challenging the misconception that isolation guarantees security.

OT is challenging to protect for several reasons

abacode

Challenges

People

- **OT security experts are difficult to hire / retain**
- **Distributed stakeholders** of OT cyber risk (E.g., security vs. operations)
- Overreliance **on individual knowledge/experience**; minimal continuity
- IT security skillsets do not match 1:1 to OT security skillsets

Process

- Overly focused on security initiatives **designed to solve point problems** without coordinating through a single office (E.g., OT PMO)
- **Decentralized approach** to OT cybersecurity across large site network
  - Differing frameworks
  - Ad hoc incident response approaches

Tech

- **Legacy systems** that are difficult to secure
- Many OT devices with **varying versions and patches**, lacking clear change management history
- **Vendor usage ad hoc** amongst sites or business units

Implication for OT security

- **Lack of coherent enterprise strategy leads to unfocused or uncoordinated security programs**
- **Risk ownership and risk management disaggregated**
- **Lack of clear metrics to "measure what matters"**
- **Inadequate sequencing/prioritization of initiatives limits impact**
- **Many vendors in the environment can introduce more risk**

The rapid convergence of IT & OT exposes vulnerable OT systems to attackers

Risk Exposure

Detailed next

	1980 - 2000 Legacy Control System Environments	2000 - 2010 Dawn of IT / OT Convergence	2010 – 2020+ Era of total connectivity
Defining attributes	• Physically isolated OT environments • Obscure / custom built control systems • Designed for operations not security	• Ethernet becomes mainstream in IT • IT / OT convergence takes off • Increased ICS remote access	• Fully connected ICS environments • Documented ICS software and protocols • Internet of Things connects the world
Implications for OT security	• Physical access is needed to impact the environment • Detailed environment research necessary for bespoke attack chains	• OT environments inherit vulnerabilities of integrated IT assets • Connected OT environments expose insecure ICS systems • Vulnerabilities can be exploited remotely	• Convenient remote operations create efficient attack vectors for threats • Easily accessible knowledge base for building ICS malware • Vulnerability fatigue clouds risk-based vulnerability management

Cyberattacks on OT environments impact critical operations and cost victims millions

Information and tool sharing has rapidly lowered the bar for attackers wishing to inflict harm

Typical losses and expenses from cyberattacks

- Cyber incident response expenses
- Recovery expenses, such as extortion by ransomware
- Extra expenses to run business, such as hiring additional staff or purchasing third-party services.
- Sales loss due to system inoperability

5 days

Average duration of a disruption caused by an ICS/OT Cyberattack

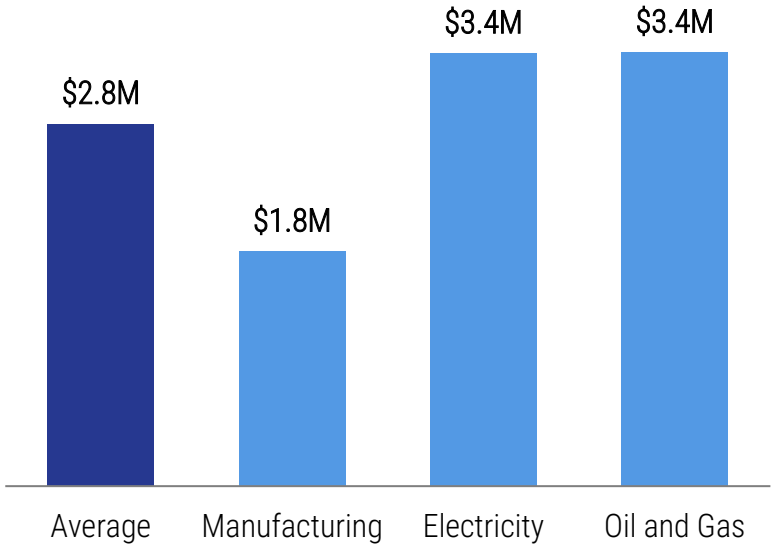
$2.8M

Average financial damages over 12 months due to ICS/ OT Cyberattack

Case Study: A tough pill to swallow

In June 2017 pharmaceutical giant Merck experienced a NotPetya ransomware attack that disrupted operations for nearly a week, leading to $135 million in lost revenue and an additional $175 million in other expenses over the next 6 months for a total disclosed loss of **$310 million**

Average Financial Damages (over 12 months)



Sources: Trend Micro - The State of Industrial Security May 2022; https://cyberscoop.com/notpetya-ransomware-cost-merck-310-million/

Getting started in your OT security journey can be as simple as asking 5 key questions

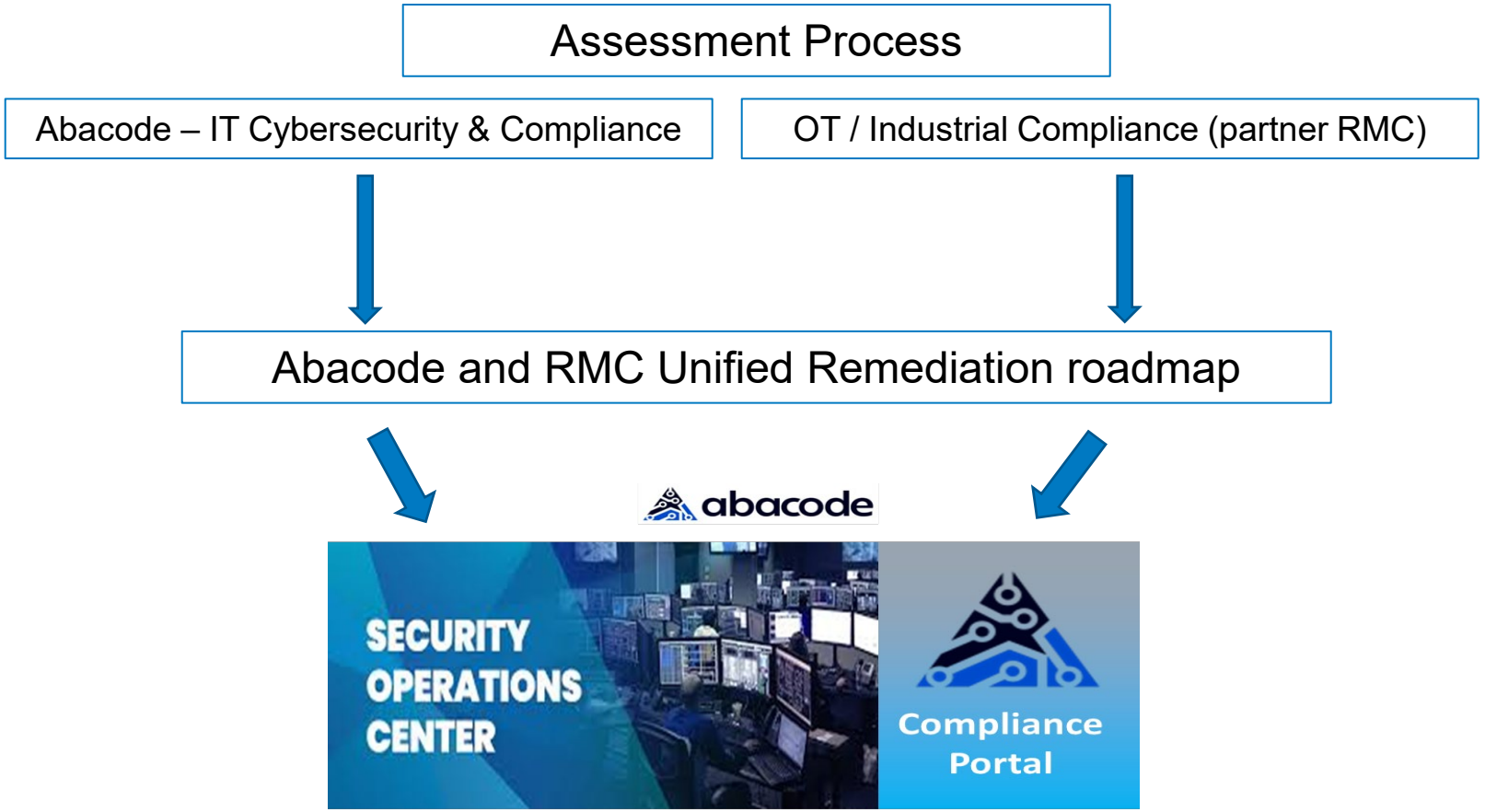
abacode

Control	Characteristics (non-exhaustive)	Key Benefits	Questions
Defensible Architecture	• Asset identification and inventory • Segmented environment • Network flow controls	• Reduced attack surface • Controlled ingress and egress • Robust data/indicator collection	**Is your organization's ICS environment accessible from the outside world?**
ICS Networking Visibility Monitoring	• Passive traffic monitoring • Heuristic based threat detection • Data collection and aggregation	• Identify malicious anomalies • Support incident investigations • Identify root cause of issues	**Can your organization define *normal* network activity within your ICS environment?**
Risk-Based Vulnerability Management	• Focused on threat scenarios • Contextual patch prioritization • Gap mitigation and monitoring	• Threat informed remediation • Balanced operational needs • Conservation of resources	**Do you know which vulnerabilities are most impactful to mitigate in your organization's ICS environment?**
Secure Remote Access	• Multi-factor authentication • Least privilege access • Isolated bastion hosts	• Forced multi-stage attack vectors • Limited access on compromise • Technical and physical hurdles	**Are engineers and third parties able to connect directly into your organization's ICS environment?**
ICS Incident Response	• Consequence based scenarios • Adversary influenced strategies • Regularly tested and evaluated	• Actionable response playbooks • Return to operation preparedness • Validated response procedures	**Are you confident your ICS incident response plans prepare your organization for an efficient recovery in the event of an attack?**

A phased approach for a manufacturing client

Focus areas

Ultimate Combined Model



- Respective Assessments
  - Abacode – IT
  - RMC - OT
- Abacode to participate in RMC Remediation plan specific to OT Monitoring
- Abacode provides IT / OT Monitoring
- RMC provides recurring / rotating on going assessments

Additional precautions for vendors to manufacturing firms and utilities

Your professional / Tech E&O liability is also on the line in the event your digital connectivity to clients introduce malware to their OT or IT systems:

- Employ DevSecOps for any software deliverables to prevent spread of vulnerabilities to clients via Remote Patching, Open-source software code, Credential harvesting, etc.
  - Perform a software composition analysis
  - Regular code reviews
  - Security testing
  - Monitor dark web for early chatter about exploits
  - Have an incident response and rollback plan to close vulnerabilities & limit impact

Use Zero Trust Remote Client Access when connecting remotely to clients

- Separation of concern between the:
- Support laptops
- Technical environment
- Environment of their clients

Disclaimer

The information provided in these materials is intended to be general and advisory in nature. It shall not be considered legal advice. The Hartford does not warrant that the implementation of any view or recommendation contained herein will: (i) result in the elimination of any unsafe conditions at your business locations or with respect to your business operations; or (ii) be an appropriate legal or business practice. The Hartford assumes no responsibility for the control or correction of hazards or legal compliance with respect to your business practices, and the views and recommendations contained herein shall not constitute our undertaking, on your behalf or for the benefit of others, to determine or warrant that your business premises, locations or operations are safe or healthful, or are in compliance with any law, rule or regulation. Readers seeking to resolve specific safety, legal or business issues or concerns related to the information provided in these materials should consult their safety consultant, attorney or business advisors. All information and representations contained herein are as of February 2023.

Certain coverages vary by state and may not be available to all businesses. All Hartford coverages and services described on this page may be offered by one or more of the property and casualty insurance company subsidiaries of The Hartford Financial Services Group, Inc. In Texas, Arizona, New Hampshire, Washington and California by Hartford Accident and Indemnity Company, Hartford Fire Insurance Company, Hartford Casualty Insurance Company, Hartford Lloyd's Insurance Company, Hartford Insurance Company of the Midwest, Navigators Insurance Company, Navigators Specialty Insurance Company, Maxum Casualty Insurance Company, Maxum Indemnity Company, Trumbull Insurance Company, Twin City Fire Insurance Company, Hartford Underwriters Insurance Company, Property and Casualty Insurance Company of Hartford and Sentinel Insurance Company, Ltd. and its property and casualty insurance company affiliates, One Hartford Plaza, Hartford, CT 06155.

**Rating determinations made by rating agencies are subject to change from time to time. While the Company attempts to show accurate information, it cannot assure the timeliness of ratings referred to herein and assumes no obligation to monitor the ratings actions of any rating agency. AM Best, S&P and Moody's ratings as of January 2023 and are on a stable outlook. A+ rating from AM Best represent the 2nd highest rating among 13 rating categories. An A1 rating from Moody's represents the 5th highest rating among 21 rating categories and an A+ from Standard & Poor's represents the 5th highest rating among 20 rating categories*

The Hartford Financial Services Group, Inc., (NYSE: HIG) operates through its subsidiaries, including the underwriting company Hartford Fire insurance Company, under the brand name, The Hartford®, and is headquartered in Hartford, CT. For additional details, please read The Hartford's legal notice at www.thehartford.com