#RSAC

RSAConference2022

San Francisco & Digital | June 6 – 9

TRANSFORM

SESSION ID: **SAT-W02**

The Cyber Physical War – Lessons From the Digital Front Line

Ian Bramson

Global Head – Industrial Cybersecurity
ABS Group

Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

Industrial Cybersecurity is Hitting a Tipping Point

Ransomware Attacks in 2021[1,2]

105%

increase Worldwide

104%

increase in North America

80%

of organizations were hit by a ransomware attack and more than

60%

of those organizations paid the ransom

Top Ransoms Paid in 2021

May 2021	June 2021
Colonial Pipeline Co. $4.4 Million	JBS $11 Million
Brenntag $4.4 Million	

Recent Attacks to Critical Infrastructure

- Oldsmar Water Treatment Facility – Feb. 2021
- German Fuel Supply Terminal – Feb. 2022
- Ukraine Attacks – Feb. and Apr. 2022
- German Wind Turbines – Feb. and Mar. 2022

High-Profile Vulnerabilities Discovered in the Last Six Months

- Log4J – Dec. 2021
- APT Cyber Tools Targeting ICS/SCADA Devices – Apr. 2022
- Pipedream Malware Toolkit Discovery – Apr. 2022

A New Priority for Governments and Trade Associations

IACS International Association of Classification Societies: UR E26 and UR E27

NIST National Institute of Standards and Technology, U.S. Department of Commerce: NIST SP 800-82r3

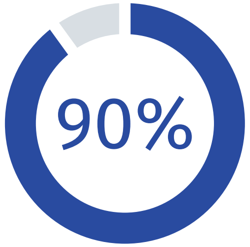
CSA Singapore: Cybersecurity Act, Part 5

Pipeline Security Guidelines Update

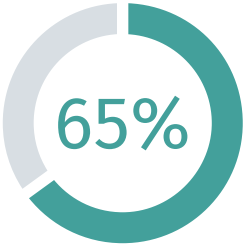
الهيئة الوطنية للأمن السيبراني
National Cybersecurity Authority: Operational Technology Cybersecurity Controls (OTCC-1:2022)

Executive Orders

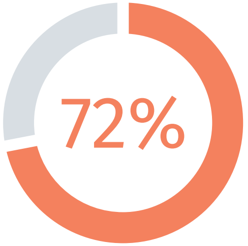
OT Cybersecurity by the Numbers



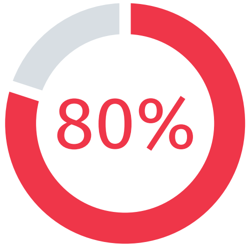
Organizations that use **OT systems** have experienced some sort **of cyber incident** in the **past year**. [3]



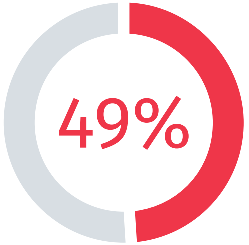
Organizations with **limited visibility** in their control systems [4]



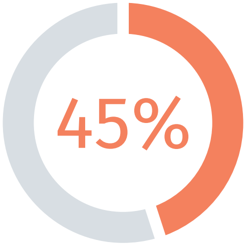
Organizations that **don't have full visibility** into their **supply chains** [5]



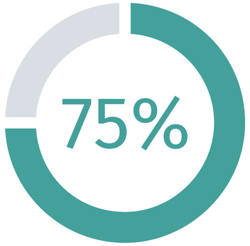
Organizations that find it **difficult to stop cyber** attacks **in time** [6]



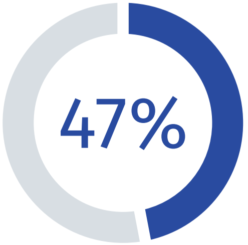
Increase in **ICS vulnerabilities** between 2019 and 2020 [7]



Organizations with **control systems at high risk** [8]



External attacker can **penetrate** the **ICS networks** at 75% success rate [9]



Organizations **without internal resources** to manage **OT/ICS incidents** [10]

RSAConference2022

Perspectives From the Digital Front Line

I Spoke to the Digital Front Line

Suppliers
& Vendors
Government
Technical
Implementors
(OT &IT)
Board
Members
Insurers

My background

- 25+ years in strategy and cyber
- 6+ years focused on industrial cyber for critical infrastructure
- 100s of conversations and engagements across all audiences
- 40+ countries

I spoke with

- Technical Experts (Analysts, Threat Hunters, Labs)
- Government (Regulators, State Governments, Standards Orgs)
- Insurance Companies (Insurers, P&I Clubs, Associations)
- Supply Chain & Manufacturing (Suppliers, OEMs, Manufacturers)
- Implementors (CISOs, Plant Managers, Service Providers)
- Board of Directors (Boards, Analysts, Executives

Technical Experts

Who we asked

- Threat Hunters
- Managed Service Analysts
- White-Hat Hackers
- Cyber Labs

What you need to know

- OT is less mature and much more exposed
- Digitization expanding the attack surface
- Risk to safety – site, public, environment
- No such thing as "air gapped"
- Almost no visibility into OT systems
- OT takes specific expertise

What you need to do

- Do the basics – Asset inventory, identity management, monitoring, response
- Know the identities that access OT systems (e.g., suppliers) and how they access them

> "I've been able to hack into an industrial site in less than eight minutes… my coffee wasn't even cold."
>
> ~ White Hat Hacker

> "Attacks like Colonial Pipeline might be a warning bell for us, but it's a dinner bell for attackers."
>
> ~ Cyber Specialist

Government Perspective

Who we asked

- Federal Agencies (CISA, USCG, TSA, DHS)
- Sate Governments
- International Governments
- Standards and Governance Organizations (e.g., IMO, NIST, NERC)

What you need to know

- Increase attacks on critical infrastructure has broad impacts on the economy, national security and political stability
- Definition of critical infrastructure expanding
- Regulations will focus more on monitoring
- Compliance does not equal security
- Supply chain risk management is key

What you need to do

- Go beyond compliance and put in what will make you secure
- Make sure you have strong monitoring, reporting and response controls in place
- Look closely at supply chain risk management

> "It is the policy of my administration that the prevention, detection, assessment and remediation of cyber incidents is a top priority and essential to national and economic security."
>
> ~ Executive Order on Improving the Nation's Cybersecurity – May 2021

Insurers Perspective

Who we asked

- Insurance Companies
- P&I Companies
- Insurance Associations
- Insurance Focused Law Firms

What you need to know

- Cyber physical events straining insurance and driving costs up
- Cyber is very hard to underwrite
- Premiums are going up significantly
- Underwriting becoming much more stringent
- Exclusions are important

What you need to do

- Read the fine print and watch exceptions
- See how policies interrelate (e.g., suppliers, pollution)
- Come prepared to underwriting sessions
- Make insurance part incident response plans

> "It will be harder to qualify for cyber insurance, and the implementation of many common cybersecurity controls will increasingly be required as a condition of coverage."
>
> ~ Joshua Motta,
> CEO and co-founder of Coalition

Suppliers Chain and Manufacturing

Who we asked

- Supply Chain and Manufacturing Executives
- OEMs
- Technology Providers

What you need to know

- Attacks can happen on the supply chain
- Attacks can happen through the supply chain
- You inherit the risk of you full supply chain
- Supply chain resiliency can work against cyber resiliency
- Most supply chains lack visibility & control

What you need to do

- Employ security by design
- Cyber map your supply chain
- Consider cyber acceptance testing

> "The pressure on building supply chain resiliency, but we don't think about cyber security when we do that…that could be disastrous."
>
> ~ Manufacturing Executive

Implementors Perspective

Who we asked

- CIOs
- Operation Mangers (e.g., plant, site)
- Industrial Cybersecurity Provider (technology and services)

What you need to know

- The digital front lines are in their networks
- Responsible for industrial cyber risk reduction
- There is often tension between IT and OT
- IT solutions will not work in an OT environment
- Technology alone cannot be the solution

What you need to do

- Create a position to lead industrial cyber
- Make sure to have domain expertise
- Build a balanced program that covers Assess and Plan, Protect and Defend, Detect and Respond

> “You can’t take an IT solution and put it into an OT environment. You might bring the network down.”
>
> ~ Operations Manager

Board of Directors Perspective

Who we asked

- Board Members
- Executives Who Present to Boards
- Market Analysts

What you need to know

- OT is the core of the business identity and revenue generation
- Risks are growing exponentially
- IT is often confused with OT
- Compliance does not equal security
- Cyber is important, but there is confusion

What you need to do

- Be clear on the Board's priorities and position
- Present cyber in a business context
- Be clear on risks and priorities
- Educate the board and dispel myths

> "Boards know cyber is a big problem. Beyond that, there's a lot of confusion."
>
> ~ Board Member
> Oil & Gas Industry

> "Most of us on the Board don't understand cyber but we do understand business and risk. Speak our language when you present to us."
>
> ~ Board Member
> Maritime Company

RSA Conference2022

The Future of OT Cyber

Prediction #1: OT cyber will overtake IT as the priority for companies

1 OT cybersecurity has a direct impact to revenue, operations, safety, brand and legal exposure

2 Increase in attacks on critical infrastructure is shifting the focus to OT

3 Companies don't want two programs and recognize OT as the more specialized field

4 Companies are asking OT cyber managed services to also provide their IT cybersecurity

So what…

- IT focused companies need to offer OT services
- CISO roles need to evolve to fully address OT
- OT will be the priority at board discussions and key to getting funding

> "They talk about OT-IT convergence. It's not a convergence, it's a hostile takeover."
>
> ~ CISO

> "The OT cyber company is covering our crown jewels in operations. We don't want two companies covering cyber, so we are asking them to cover both."
>
> ~ Senior Executive, Power & Energy

Prediction #2: Companies will buy services, not technologies

THE GLOBAL INDUSTRIAL CYBERSECURITY MARKET SIZE IS EXPECTED TO REACH

$22.8 BILLION BY 2026

according to KBV Research

- First wave of solutions - OT Technology
- Customers ill-equipped to apply technology
- Too many solutions, confuse customers
- Need is shifting to manages services
- OT takes domain expertise

So what…

- OT technology companies and OT managed services will need to form strong partnerships
- Customer solutions will include both services and solutions
- Technology sales without services will constrict to larger customers

> "Technology is not enough, without someone who knows what to do with it. It's just an expensive paperweight."
>
> ~ Executive, Power & Energy

> "We don't have the manpower, expertise or resources to handle this. We need a partner."
>
> ~ Executive, Maritime

ABS Group

Prediction #3: Market drivers will be more important than regulations

Insurance

Proposal Assessments

M&A Due Diligence

Market Valuation

So what…

- Position industrial cyber as competitive advantage
- Make OT cyber part of RFP assessments
- Conduct maturity assessments to make sure you rate highly

> “Compliance motivates you to do the least, competition motivates you to do the most.”
>
> ~ Executive, Oil & Gas

> “What if there was some sort of Moody’s rating or credit score for OT risk? That would impact valuations and drive change.”
>
> ~ OT Analyst

RSAConference2022

Conclusions

Applying OT Cyber

Do Now

- Conduct a Maturity Assessment and Build a Roadmap that fits your risk environment, strategic goals and budget realities
- Develop and incident response plan
- Resolve any potential IT-OT conflicts
- Understand where your regulatory environment is heading
- Get senior management and/or the Board involved in your industrial cybersecurity

Do Next

- Hire a head of OT cybersecurity
- Put the basics in place for your OT Systems
  - Asset Inventory and Management
  - Vulnerability Management
  - Monitoring and Response
  - Training
- Report to the Board or senior management regularly
- Consider cyber insurance to augment your program

Sources

- [1] Fortune.com – There's a huge surge in hackers holding data for ransom, and the experts want everyone toa take these steps
- [2] Forbes - A Majority Of Surveyed Companies Were Hit By Ransomware Attacks In 2021—And Paid Ransom Demands
- [3] 2021 The State of Operational Technology and Cybersecurity – Fortinet
- [4, 8,10] 2022 SANS Survey – Threat-Informed Operational Technology Defense: Securing Data vs. Enabling Physics
- [5] Industry Week—Can't Turn Back Time: Cybersecurity Must Be Dealt With—2017
- [6] Gartner—Market Guide for Managed Security Services—2020
- [7] Forbes X Force Threat Intelligence index—2021
- [9] Help Net Security— The cybersecurity of industrial companies remains low, potential damage can be severe—2021