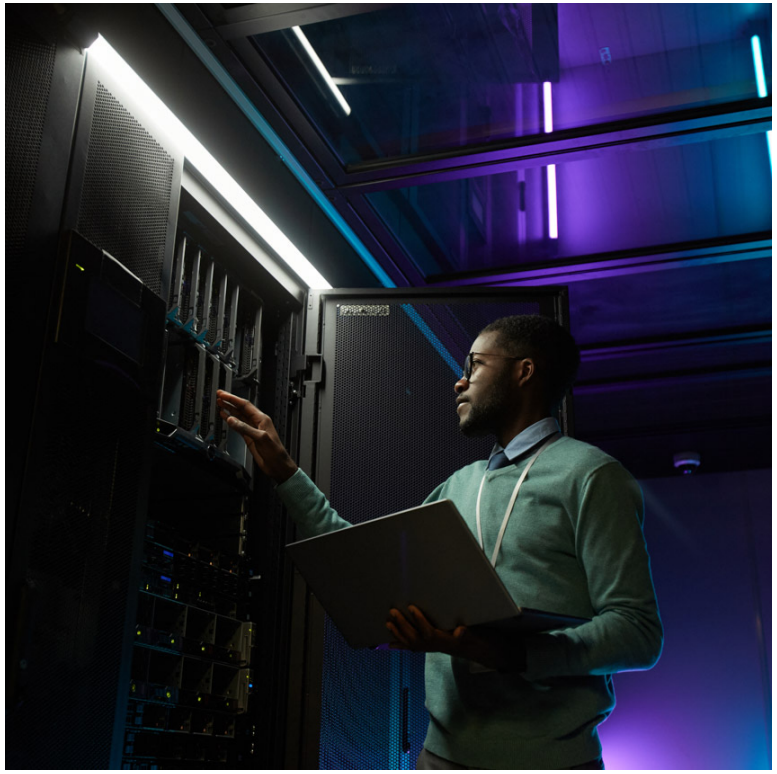
# Maintain Your Intelligent Assets or Pay the Price

Kristian Steenstrup



Gartner®

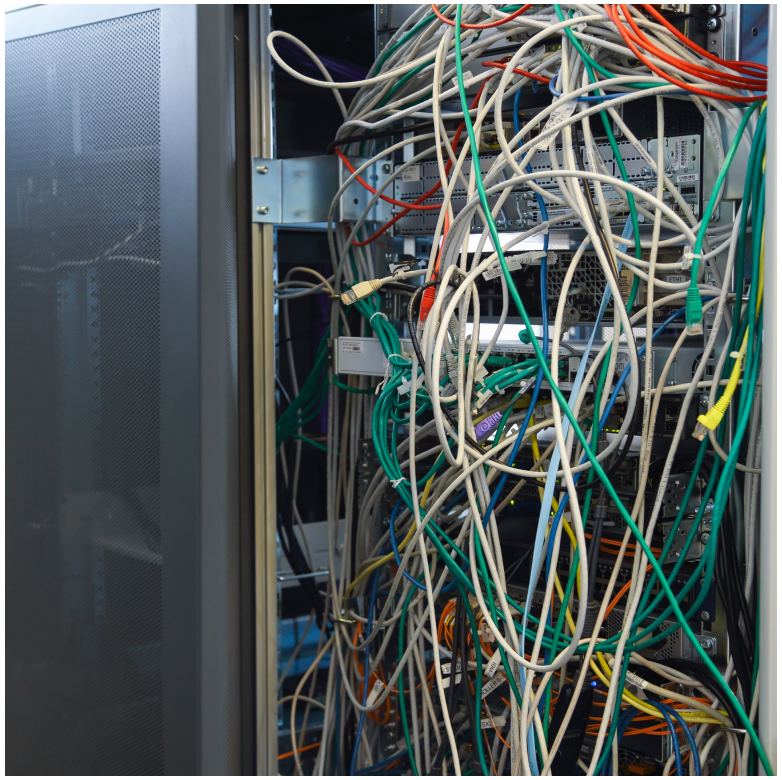
# What You Think Intelligent Assets Look Like

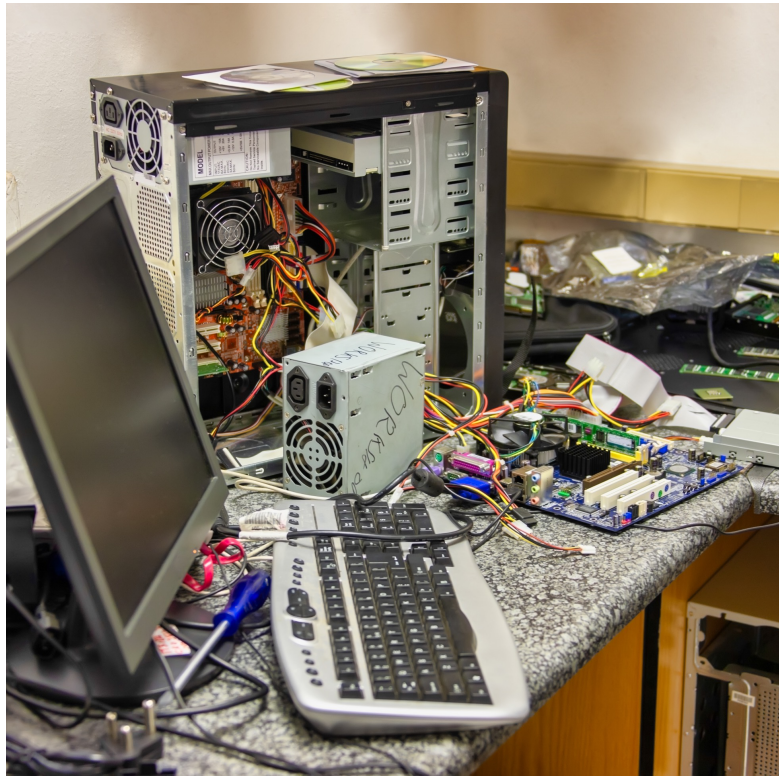





Gartner®

# What Intelligent Assets Actually Look Like








Gartner®

# Underlying Causes of the Problem




Gartner®

# Intelligent Assets Live in 2 Different Worlds

| | Information Technology | Intelligent Assets (IoT and OT) |
|---|---|---|
| **Purpose** | Managing information, automate business processes | Managing assets, controlling plant processes |
| **Organization** | **Centralized** in one department | Sometimes **dispersed and fragmented** across operational lines of business |
| **Governance** | **Clear IT governance** with the CIO in charge of the planning, acquisition, deployment and support of IT | **No single authority** ensuring use of standards, architecture plan or authorization of new developments, resulting in many stand-alone OT systems |
| **Tools and Methods** | **Transactional** data-recording, information-processing, publishing and collaboration platforms | **Event-driven,** real-time observation and control of physical events, embedded software and rule engines |
| **Talent** | CIO, infrastructure, operations and applications professionals | Engineers, technicians, and line of business managers |
| **Vendors** | IBM, Amazon Web Services, Oracle, Microsoft, SAP, Salesforce, Google, etc. | Siemens, Schneider Electric, Caterpillar, General Electric, ABB, KUKA, Schindler |




Gartner®

# Cultural Differences Undermine Efforts

**Culture of IT:**

- Manage frequent change
- Shorter lifetimes for products & systems
- User/customer convenience
- “The user experience”

**Solution Approach:**

- Develop/use standards
- Assess requirements
- Build/buy best fit at lowest cost
- Plan for upgrades and support

**Legacy** … Is the Opposite of … **Good**

**Culture of Engineers:**

- Reliability and safety
- Fault tolerance
- Determinism
- Consistency
- Longevity

**Solution Approach:**

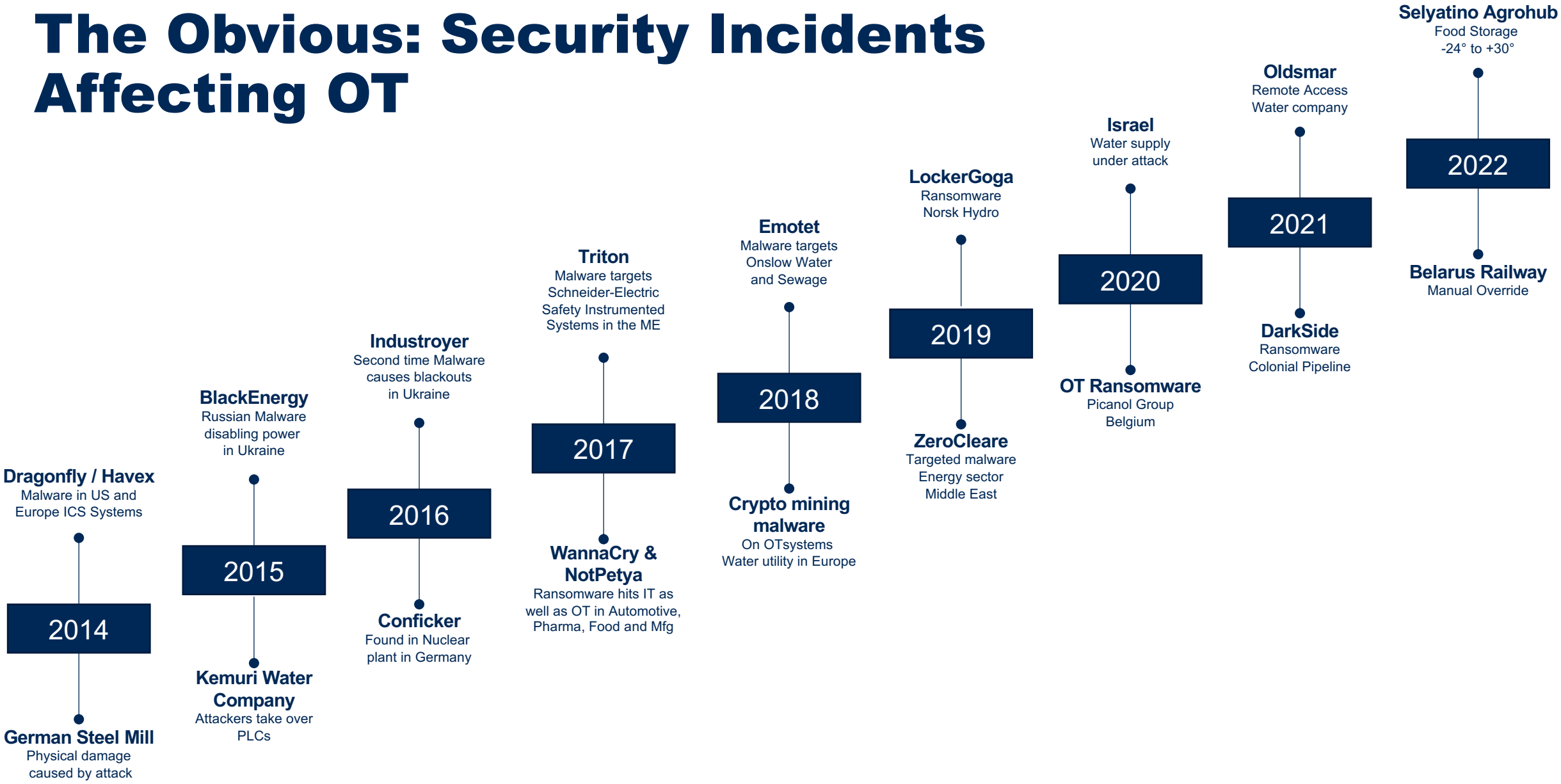
- Find example
- Iteratively optimize for performance and use
- Lockdown design
- Stability

**Change** … Is the Opposite of … **Good**




Gartner®

# The Obvious: Security Incidents Affecting OT







Gartner®

# 9%

## Of Respondents Have Experienced a Security Incident That Crippled Operational Systems But Not IT Systems

n = 398; All Respondents, Excluding Don't Know

Q: What OT security failure experiences have you had in the last year?
Source: 2021 Gartner IT/OT Alignment and Integration Survey




Gartner®

# Security Is Just One Avenue to Failure

- No Disaster Recovery
- Incorrect Software Release
- Software Incompatibility
- Technology Update Faults

# The Price of Failed Intelligent Assets

- Operator Safety
- Environmental Damage
- Direct Revenue $$$ Loss
- Product Quality
- Consumer and Partner Trust
- Competitive Position
- Brand Reputation
- Technical Debt




Gartner®

# Why Is IoT / OT Fragile?




Gartner®

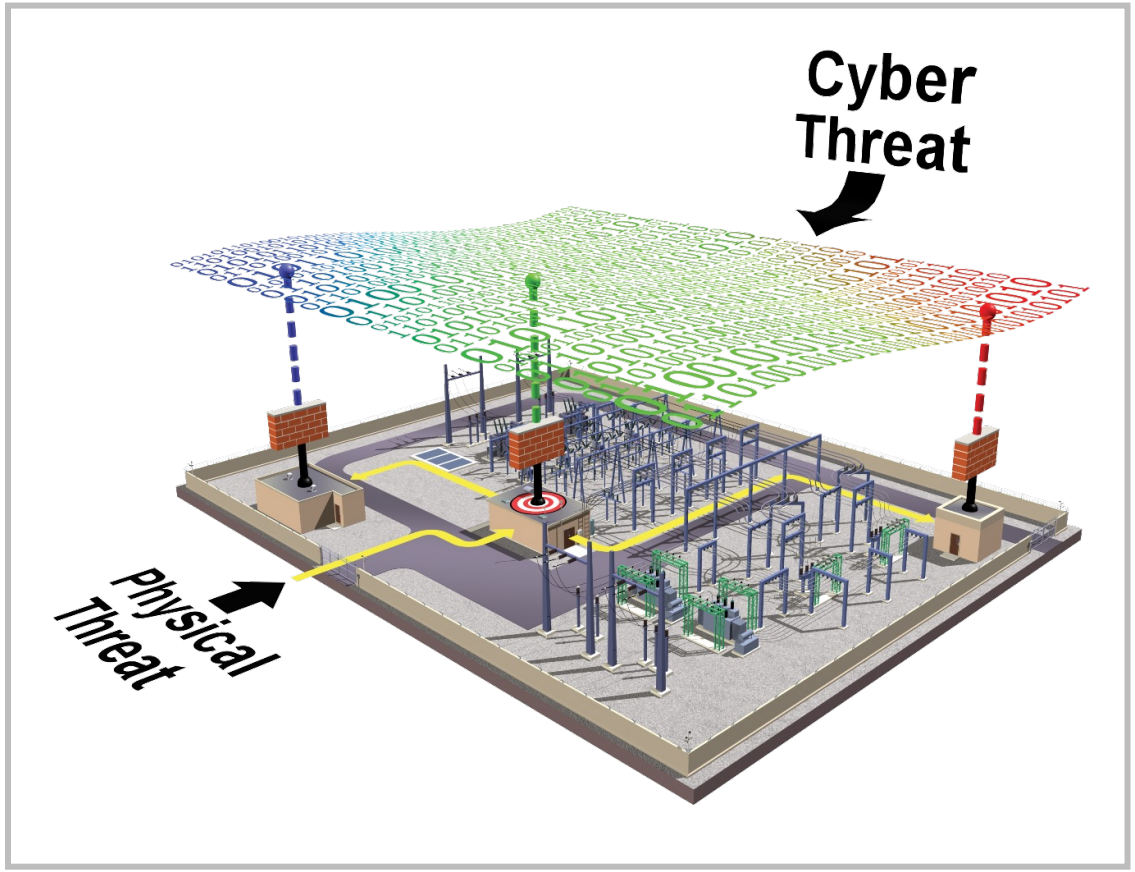
# Intelligent Assets Have Unique Security Needs

## Typical Asset Characteristics:

- Physically Accessible
- Heterogeneous
- Continuous
- Disconnected

## Basic Principles May Not Apply:

- Firewalls?
- Patch and Upgrade?
- Virus Scan?







Gartner®

# Insecure, Obscure, or Just Complicated Supply Chain

# Mounting Technical Debt

**Definition:**
Lingering software, code, hardware or other outdated infrastructure but still part of the operations stream.


**Flights Canceled:** 16,700
**Cost to Carrier:** $725 Million — $825 Million

## PROs

- Low Maintenance Cost
- Established Integration
- Familiarity

## CONs

- Strategic Incompatibility
- Outdated Support Skills
- Restricted Functionality
- Scalability
- Security




Gartner

# 6 Actions to Better Manage Intelligent Assets



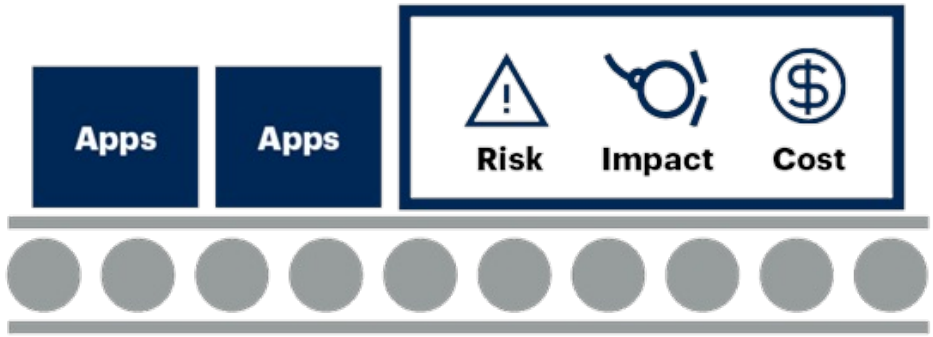

Gartner®

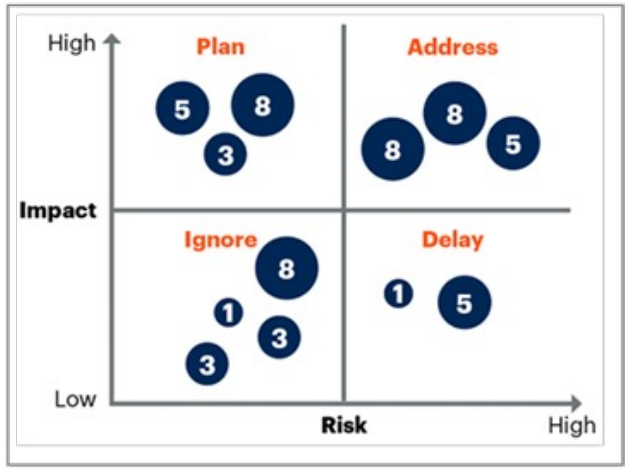
# 1. Manage Technical Debt

1


2

Use the Plan Address Ignore Delay (PAID) Model to Prioritize Technical Debt




Source: Address Technical Debt With Gartner's PAID Model and Avoid Bankrupting Your Application's Future (G00719923)




Gartner

# 2. Have IT Learn From Their Engineer Friends

- Physics matter
- Real time, means real time
- Learn to live with the old
- Every problem is a value/risk/cost problem
- Cybersecurity is physical security
- Things wear out

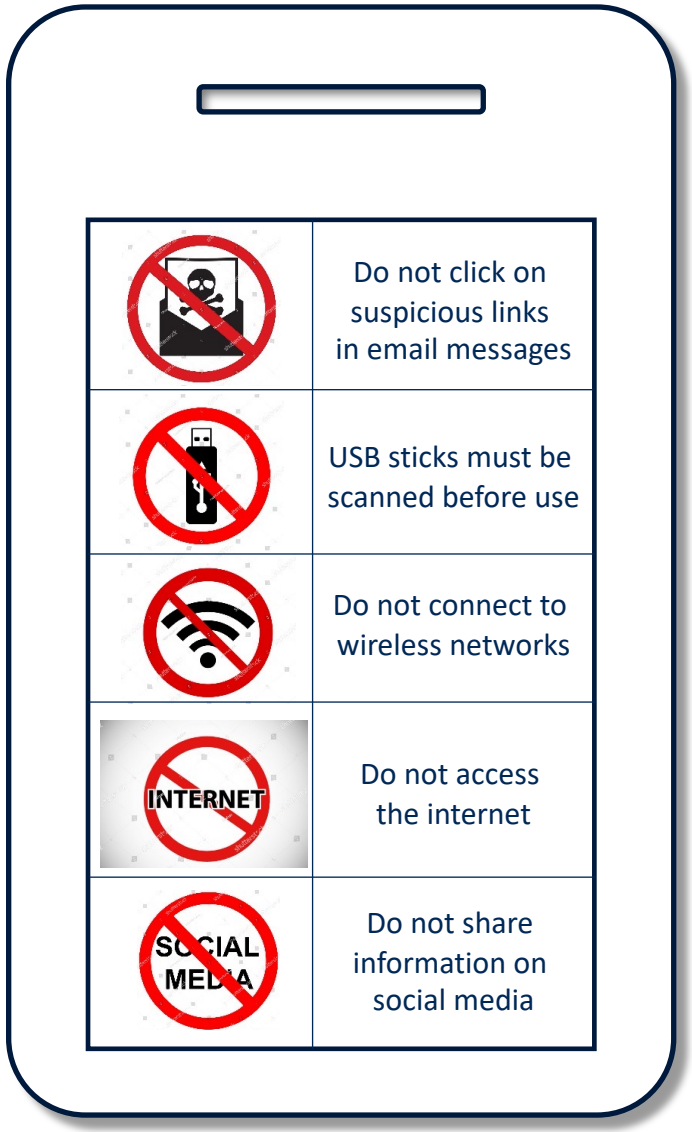




Gartner

# 3. Have Engineers Learn From Their IT Friends

- Governance and policy can be your friend
- Software impacts stability, putting safety and reliability at risk
- Use tools and processes to manage constant software change



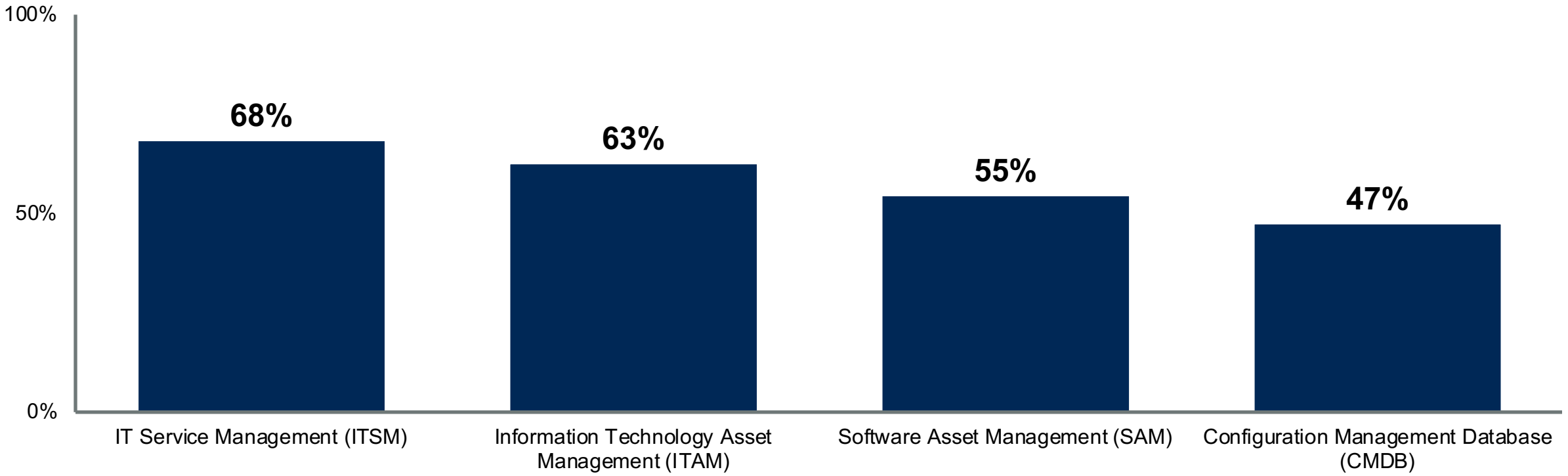




Gartner®

# 4. ITSM and ITAM Used to Manage OT Software

## Specialized Tools Used to Manage OT Software
Multiple Responses




n = 398; All Respondents, Excluding None

Q: Which of the following specialized tools are used to manage OT software in your organization?

Source: 2021 Gartner IT/OT Alignment and Integration Survey




Gartner®

# 5. Combine Physical and Software Maintenance

OT/IoT software maintenance is constrained by the real world

**Continuous Usage**

**Safety**

**Physical Access**

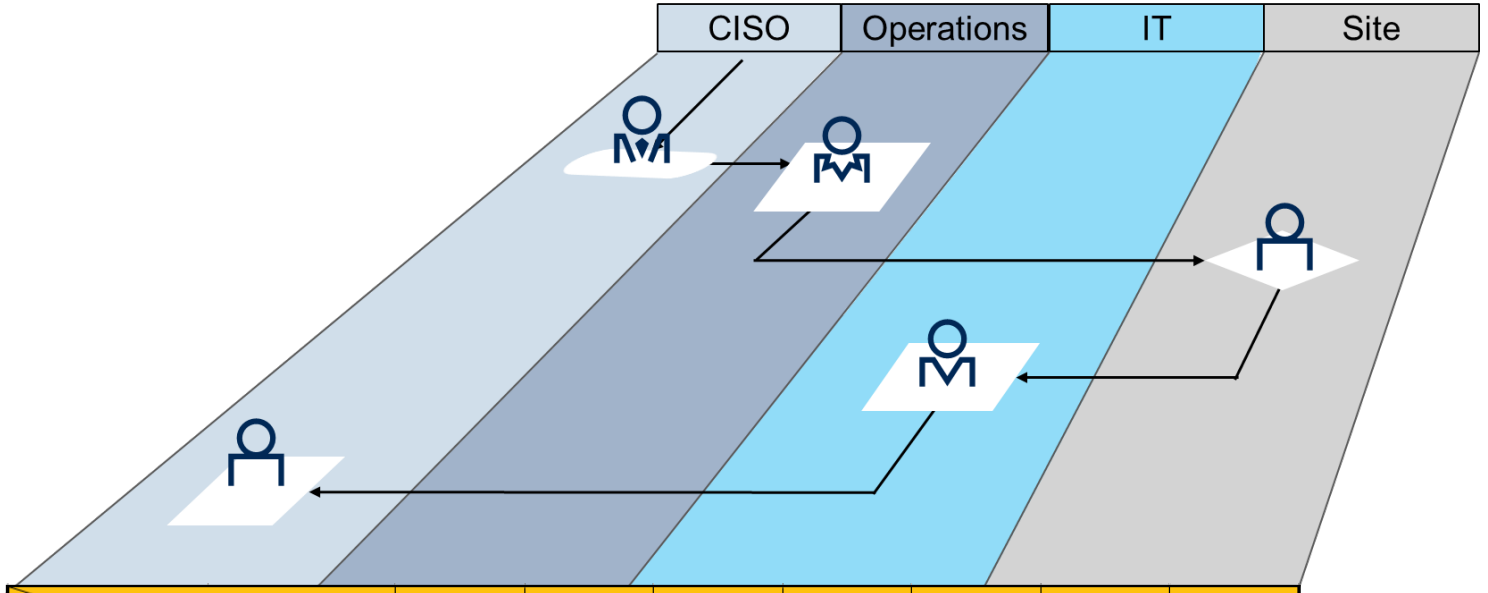
- EAM/CMMS is used for the physical equipment.
- ITAM/SAM is used for software.
- Scheduling of maintenance needs to combine physical and software maintenance.




Gartner®

# 6. Define Roles and Responsibilities

- All sites must have an accountable person for OT security appointed.
- Roles and responsibilities for all security roles must be clearly described and assigned.




| Actor \ Action | Overall Coordination | Gather Logs and Analyze | Issue Emergency Change Management | Staff Monitoring and Investigation | Staff Messaging | Senior Management Liaison | Post-Incident Report |
|---|---|---|---|---|---|---|---|
| CIO/CISO | A | | I | I | AR | AR | I |
| Incident Coordinator | R | I | A | I | C | R | AR |
| Security Operations Team | I | R | R | | | | CI |
| Internal Investigations | I | AR | C | AR | | I | CI |
| Customer Operations Center | I | | I | | I | I | C |

| | |
|---|---|
| Responsible: | Person or function that is responsible for executing the activity |
| Accountable: | Person or function that owns the activity, approves work and is held accountable for it |
| Consulted: | Person or function that has information relevant to the activity |
| Informed: | Person or function to be informed of progress and results |

# Recommendations

- Assess your OT/IoT portfolio with the help of operations.
- Include security aspects but be aware of other contributing factors.
- Cross pollinate cultures between IT and operations/engineering.
- Develop the use of integrated planning for physical and software maintenance.
- Make OT/IoT security and maintainability part of vendors obligations.
- **Prepare your disaster recovery**




Gartner®

# Recommended Gartner Research

- **To Enable Intelligent Industrial Assets, Strengthen These Digital Capabilities**
  Rich McAvey and Lloyd Jones
- **Quick Answer: What Are Intelligent Assets and Why Are They Important?**
  Rich McAvey, Lloyd Jones and Alfonso Velosa
- **When Does a CIO Need to Be Involved in OT?**
  Kristian Steenstrup
- **Quick Answer: What Should Be Included in an OT Standards Framework?**
  Kristian Steenstrup
- **As IT and OT Converge, IT and Engineers Should Learn From Each Other**
  Kristian Steenstrup and Earl Perkins
- **How to Improve Infrastructure Fitness and Sustainably Reduce Technical Debt**
  Roger Williams, Daniel Stang and Mark Margevicius






Gartner®