CYBERSECURITY THREATS TO CHEMICAL/MANUFACTURING

Are You at Risk?

INTRODUCTION

Our increasing dependence on technology and web-based communication has opened the door for cybersecurity threat, and the chemical and manufacturing sectors are prime targets. Successful attacks on chemical and other manufacturing facilities and systems can disrupt services and operations and endanger entire populations. With the growing number and sophistication of cyber attacks, securing access to sensitive information and hazardous substances has never been more important—or necessary.

WHAT ARE THE CONSEQUENCES?

- Plant Sabotage/Shutdown
- Intellectual Property Theft
- Physical Hazard/Material Spill
- Overpressure/Expansion/Explosion
- Exposures/Health Issues from Releases beyond Plant Limits

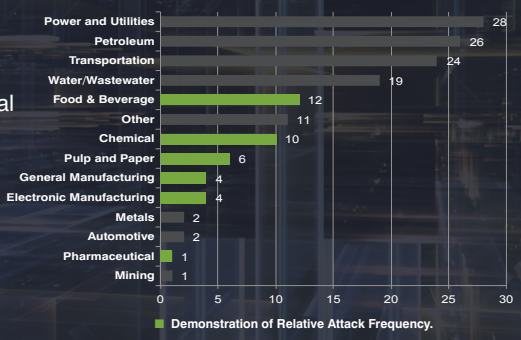
WHAT THREATS DO YOU FACE?

96% of all security incidents fall into nine basic patterns:

1. Point-of-Sale Intrusions
2. Crimeware
3. Cyber Espionage
4. Insider Misuse
5. Web App Attacks
6. Miscellaneous Errors
7. Physical Theft/Loss
8. Payment Card Skimmers
9. Denial of Service

HOW DO YOU RANK?

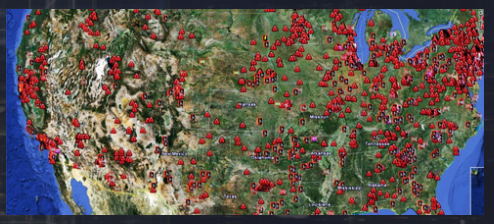
MOST TARGETED INDUSTRIES (GLOBAL)



Source: Repository of Industrial Security Incidents/Security Incidents Org.

WHAT IS INDUSTRIAL ESPIONAGE?

Industrial espionage is spying with the intent of learning the secrets or sensitive information of an industrial competitor for commercial or other gain. At-risk documents include design documents, formulas, and manufacturing processes, which can disclose information on gaps in an organization's process or structure.



In the United States alone, 7,200 key industrial control systems are directly linked to the Internet and are vulnerable to attack.
Source: US ICS-CERT

WHAT'S REQUIRED?

- **HSPD-7** requires the strengthening of the security and resilience of critical infrastructure against cyber threats that could have a debilitating impact on national security, economic stability, or public health and safety, including acts of terrorism.
- **CFATS** identifies and regulates high-risk chemical facilities to ensure that they have the necessary security measures to avoid attack or exploitation.
- **Executive Order 13650** improves chemical facility safety and security in coordination with owners and operators.
- **NERC CIP** defines industrial cybersecurity standards, focusing on system reliability and customer information security.

WHAT SHOULD YOU PROTECT?

UTILITIES AND OFF-SITES | MANUFACTURING FACILITIES | PIPELINES | MANUFACTURING PROCESSES | CONFIDENTIAL INFORMATION

PARSONS

IT COULD HAPPEN TO YOU

2006 (ONGOING) — Shady RAT, a series of professional-grade cyber attacks, compromised control of computers at dozens of commercial and government organizations in the chemical/industrial sector.

2010 — STUXNET, a sophisticated malware, halted uranium enrichment at a nuclear facility in Iran during a sustained 2-year attack.

2011 — Trojan virus Poison Ivy was used to collect intellectual property from 29 international chemical companies in one of the largest industrial espionage attempts in history.

2014 — German steel mill received massive damages after cyber manipulation and disruption of control systems prevented a blast furnace from shutting down properly.

2014 — Malware Shamoon wiped 30,000 workstations in Saudi Aramco's corporate network, raising concern toward cyber attacks that can bypass firewalls to affect operations technology networks.

WHY PARSONS FOR CYBERSECURITY?

Parsons has worked behind the scenes for 30+ years to deliver cybersecurity services that have protected our nation's most sensitive information and critical infrastructure to federal customers. This experience is enhanced by 70+ years of experience designing, building, and managing these assets around the globe. Parsons has combined its in-depth knowledge of cybersecurity with its expertise in the sustainment of critical assets to offer PARSecure®, a secure suite of services that includes both cyber and physical security. This offering allows us to leverage our experience and become a trusted cybersecurity partner for customers in federal, state, and local government, and the commercial marketplace. Using PARSecure® and our team of cybersecurity experts, we can ensure that cutting-edge cybersecurity people, processes, and technologies are in place—addressing the full spectrum of risks to your business and protecting your most valuable assets.

Setting us apart is our state-of-the-art Cyber Solutions Center, located in Centreville, VA. This hands-on laboratory enables the Parsons team to demonstrate and analyze operational networks, supervisory control and data acquisition (SCADA) systems, and industrial control systems (ICS) that control all critical infrastructure, building systems, manufacturing systems, medical treatment facilities, water and wastewater, transportation, and more. We can then custom design, test, and implement the technical options needed to protect the security of client networks and infrastructure, in addition to providing training to those entrusted to maintain the security of these systems.

Parsons is a leader in technical solutions, continuity of operations, critical infrastructure, and classified facility protection. Together, we create a safer, more secure world.

OUR CAPABILITIES

ASSESSMENTS
Vulnerability Assessments
Certification and Accreditation
Penetration Testing

ANALYSIS & PLANNING
Security Assessments
Analysis
Remediation Plan Development

DESIGN
Plans/Policies Development
Network Security/
Security Monitoring Design

IMPLEMENTATION
Software Development
Software Tool Procurement
Security Solution
Development/Integration/Testing

OPERATIONS/MAINTENANCE
Operational Assurance
Incident Response Management
Continuous Security Improvement
External Stakeholder Coordination

CONTACTS

Jay Williams
ICS/SCADA Cybersecurity
Business Development Director
(315) 706-7154
jay.williams@parsons.com

Bob Talbot
ICS/SCADA Security Solutions Manager
(703) 679-9187
robert.talbot@parsons.com

Bill Hughes
Chemical/Industrial
Vice President
(216) 509-0668
bill.hughes@parsons.com

Design–Build–Protect

For more information or to request a demo, please go to:

www.parsons.com/cyber

EXIM APPROVED Parsons #021 29 Jul 15