



**VERSPRITE**

# **Offensive Threat Models Against the Supply Chain**

# Defining Supply Chain



Raw Materials

Raw materials are sourced from multiple global locations



Components

Raw materials used to make parts found in products



Manufacturing

**Manufacturers assemble products using components from various sources**



Retail

Web, store retailers sell manufactured goods to consumers



Consumerism

Consumers use products in home & businesses

# Supply Chain Threat Models Blueprints for Security

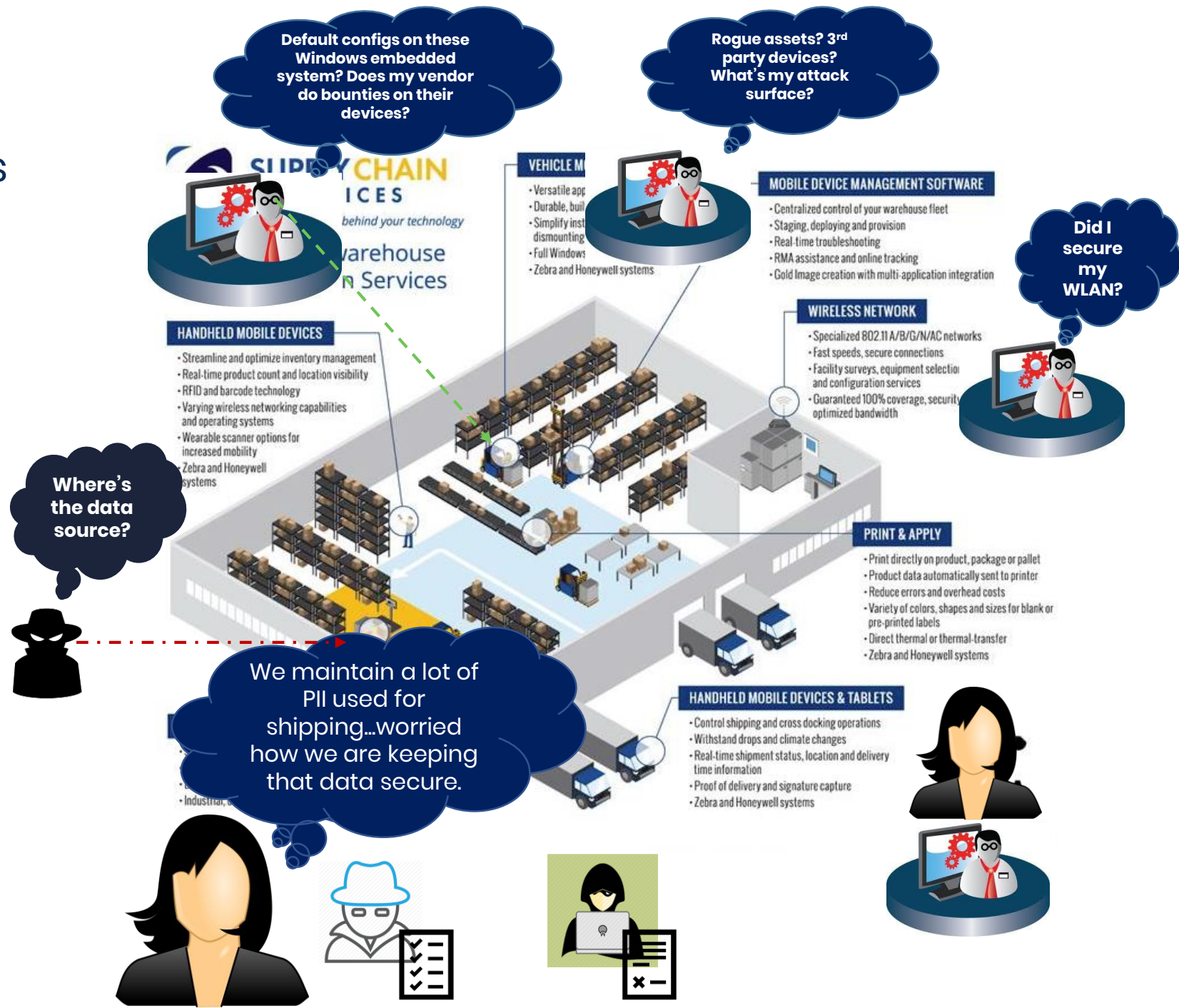
**Security Blueprint encompasses multiple security/IT disciplines:**

- Regulatory Risk Reviews/ Prior Risk Assessments
- Business Impact Analysis
- Asset Management
- Security Hardening
- Security Architecture Review
- Threat Analysis
- Vulnerability Assessment
- Penetration Testing
- Residual Risk Analysis

## Threat Modeling

### Weaknesses ≠ Threats

- Inverse of a CWE or CVE ≠ Threat





# General Motives & Probabilistic Analysis



## Threat Motives

Intent

Rewards

Repudiation



## Probabilistic Analysis

Access

Risk Aversion of Threat Agent

Capabilities

# Impact Considerations

1

## Financial Loss

Lost sales, charges run up by criminals using enterprise resources billed to the company, increased insurance premiums, fines /penalties for unreported breaches, costs of upgrading security, etc) –

**Average cost of an attack is \$1.1 million**

2

## Time Loss

Businesses estimate it takes over 60 hours to respond to a software supply chain attack.

3

## Cargo Loss (COGs Loss)

3-5 times the value of the cargo, all told, because of opportunity cost of replacement, disruption to schedules, etc.

4

## Associated Losses (Corporate)

Loss of customer trust  
reputational harm  
Loss of market share/market cap

5

## National Security

Threats when the targets are strategic assets (mail service, power grids, trains/roads)

6

## Human Life/ Societal Loss

Could result in deaths if people can't reach 911 or other vital resources can't be dispatched to emergencies

# Supply Chain Threat Library & Motives

## Threat Library

Disruption

Frameup – act of framing someone

**Sabotage**

Extortion

Espionage

Data Exfiltration

Intellectual Property

Sensitive Data

Non-sensitive Data

## Threat Motives

Lulz, Practice for another target

Misdirection – blame adversary

**Reduce credibility; revenge; disgruntlement**

Financing

Obtain intel

Leverage Data for it Value




Shorten Product Development cycles


Leverage PII for Impersonation, OSINT


Intel of pattern


# World Economic Forum 2019 Risk Census

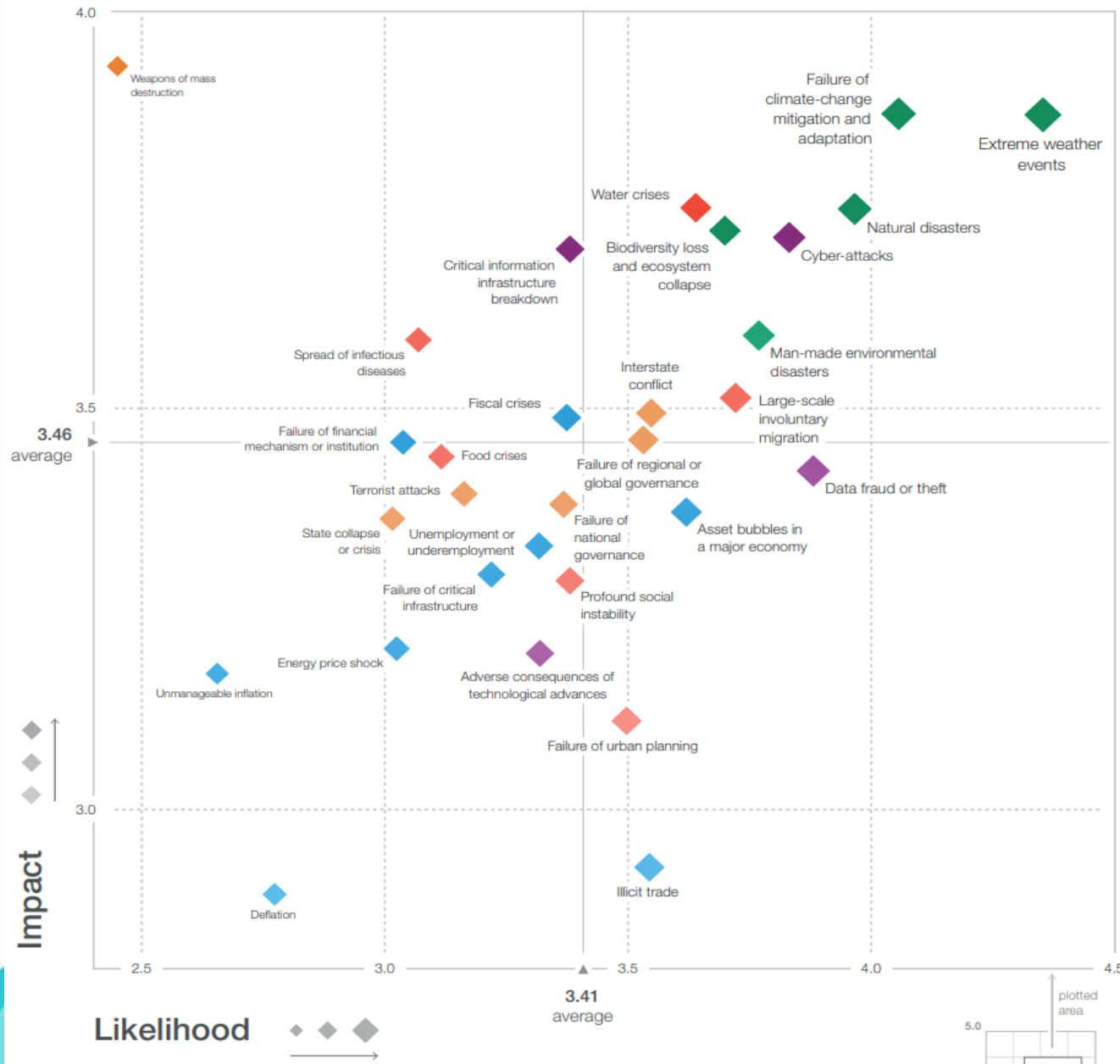
Surveys reflect escalating threats observed by 1,000 decision-makers from the public sector, private sector, academia and civil societies



 All can be impacted by supply chain focused threats and attack patterns

 Supply chain threats in these risk areas can be sanctioned by competing nation states aiming to create instability in the region.

 Supply chain threats in these risk areas can be intended as attack vectors where malicious payloads are introduced into critical infrastructure.

 Supply chain threats in these risk areas can preface other risks related to social infrastructure, financial markets, leading industries, & overall economy.



# Global Risk Interconnections (2019)

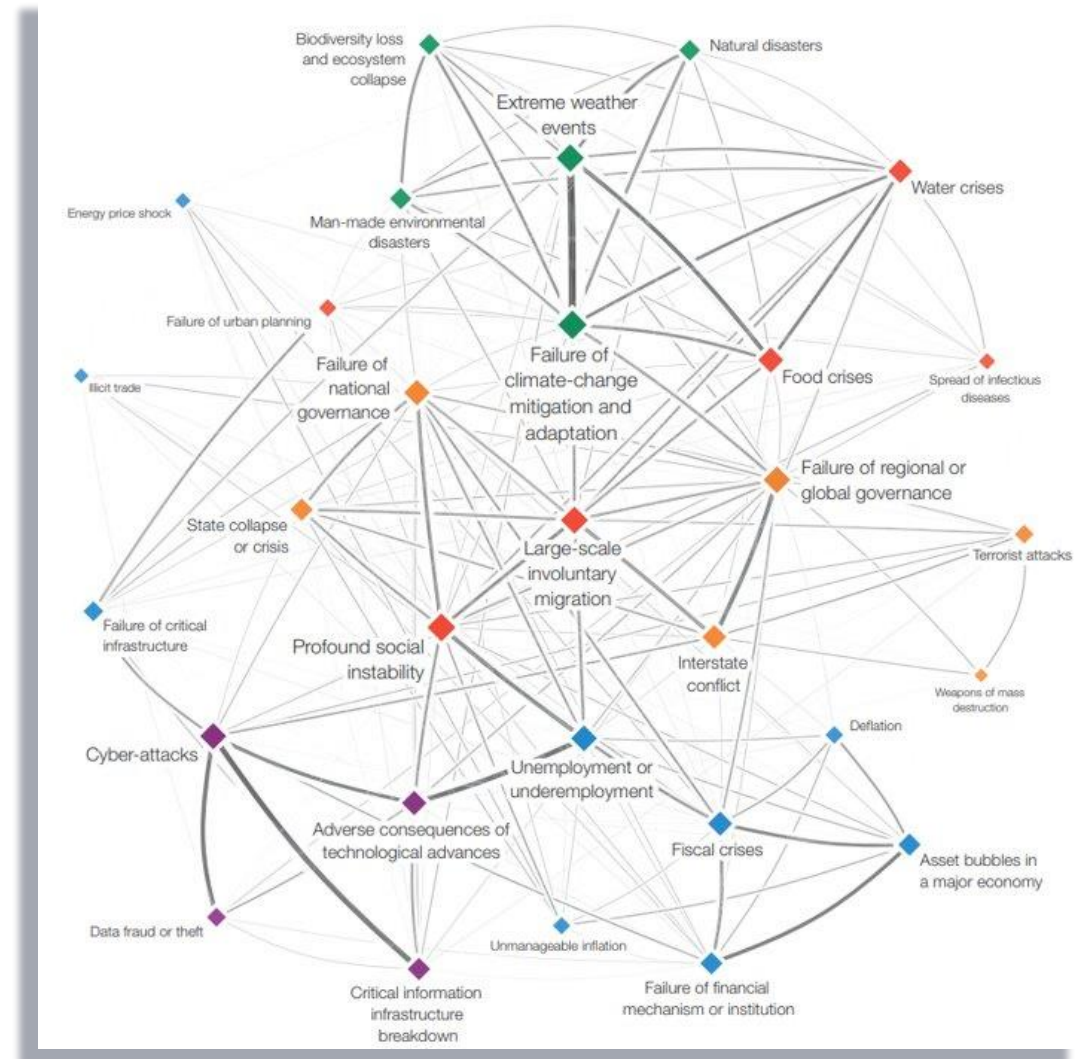
## Risks Become Interlinked

Supply chain-based threats look to usher in more long term, covert operations

Layered attacks can begin with persistence or intelligence gathering

Subsequent attack layers can expand to releasing realizing multiple types of strategic attack patterns:

- Extortion by cyber-criminal groups
- Denial of service by rival governments, interest groups
- IP theft from rising global competitors
- Info contamination in order to change public opinion





# Threat Models & Likelihood



- For supply chain, look at **correlated** risks with **high likelihood**
- Determine what part of your attack surface is relevant to the threat
- Identify vulnerabilities/ weaknesses that live within your attack surface
- Build a threat library based upon likely motives
- Build an attack library that realize motives in your threat library
- Determine success of attack patterns via security research or manual exploit testing

Top 5 Global Risks in Terms of Likelihood

	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019
1st	Asset price collapse	Asset price collapse	Storms and cyclones	Severe income disparity	Severe income disparity	Income disparity	Interstate conflict with regional consequences	Large-scale involuntary migration	Extreme weather events	Extreme weather events	Extreme weather events
2nd	Slowing Chinese economy (<6%)	Slowing Chinese economy (<6%)	Flooding	Chronic fiscal imbalances	Chronic fiscal imbalances	Extreme weather events	Extreme weather events	Extreme weather events	Large-scale involuntary migration	Natural disasters	Failure of climate-change mitigation and adaptation
3rd	Chronic disease	Chronic disease	Corruption	Rising greenhouse gas emissions	Rising greenhouse gas emissions	Unemployment and underemployment	Failure of national governance	Failure of climate-change mitigation and adaptation	Major natural disasters	Cyber-attacks	Natural disasters
4th	Global governance gaps	Fiscal crises	Biodiversity loss	Cyber-attacks	Water supply crises	Climate change	State collapse or crisis	Interstate conflict with regional consequences	Large-scale terrorist attacks	Data fraud or theft	Data fraud or theft
5th	Retrenchment from globalization	Global governance gaps	Climate change	Water supply crises	Mismanagement of population	Cyber-attacks	High structural unemployment or underemployment	Major natural catastrophes	Massive incident of data fraud/theft	Failure of climate-change mitigation and adaptation	Cyber-attacks

# Supply Chain Risks & AppSec

Business interruption topping cyber related incidents

Top Industries Affected:

- Utility/ Energy
- Transportation
- Media/ Communication
- Financial Trading
- Healthcare
- Municipalities/ City Governments

Importance of building proper threat library for  
AppSec environments in aforementioned sectors

## ALLIANZ RISK BAROMETER 2019

Top global risks facing businesses

1. Business interruption
2. Cyber incidents
3. Natural catastrophes
4. Changes in legislation
5. Market developments

Bloomberg

## ALLIANZ RISK BAROMETER 2019

Top global risks facing businesses

6. Fire, explosion
7. New technologies
8. Climate change
9. Loss of reputation or brand value
10. Shortage of skilled workforce

Bloomberg

Source: Annual 2019 Allianz Risk Barometer Report



**VERSPRITE**

# Sample Threat Models



# USPS Threat Model



- The U.S. **postal** service handles more **mail** than any other **postal** system in the world
- Retail network is larger than McDonald's, Starbucks and Walmart combined
- Traditionally, the largest provider of last mile delivery in the U.S

# Threat Model Overview

## Threats

-  Establish Persistence
-  Exfiltrate PII
-  Harvest employee info
-  Extortion
-  Cryptojacking
-  Sabotage

## Threat Motives

- Establish persistence across multiple sites in order to leverage infrastructure for multiple objectives.
- Siphon out PII from analytics platforms in order to harvest and share on black market forums.
- Collect USPS user info for the purposes of perpetration & illicit access to USPS systems.
- Hold hostage systems that are responsible for fulfillment of key processing activities, generally via ransomware.
- Obtain unauthorized access to infrastructure in order to mine crypto currency.
- Disrupt operations, particularly in areas where there is a single point of failure in order to interrupt USPS services


























## Attack Surface

-  Employees/ Contractors
-  Endpoints
-  Informedelivery.usps.com
-  Mail Sorters
-  Domain Controllers
-  AFCS Systems
-  Email
-  Network

## Associated Attack Patterns

- Collusion | Insider Threat
- Drive-by-Download | Phishing
- Injection Based Attacks | Auth Bypass
- Supply chain compromise | Malicious component
- Pass the Hash Auth Attacks
- Supply chain compromise | Malicious component
- Phishing attacks
- Network MITM | Botnets

## Associated Threats

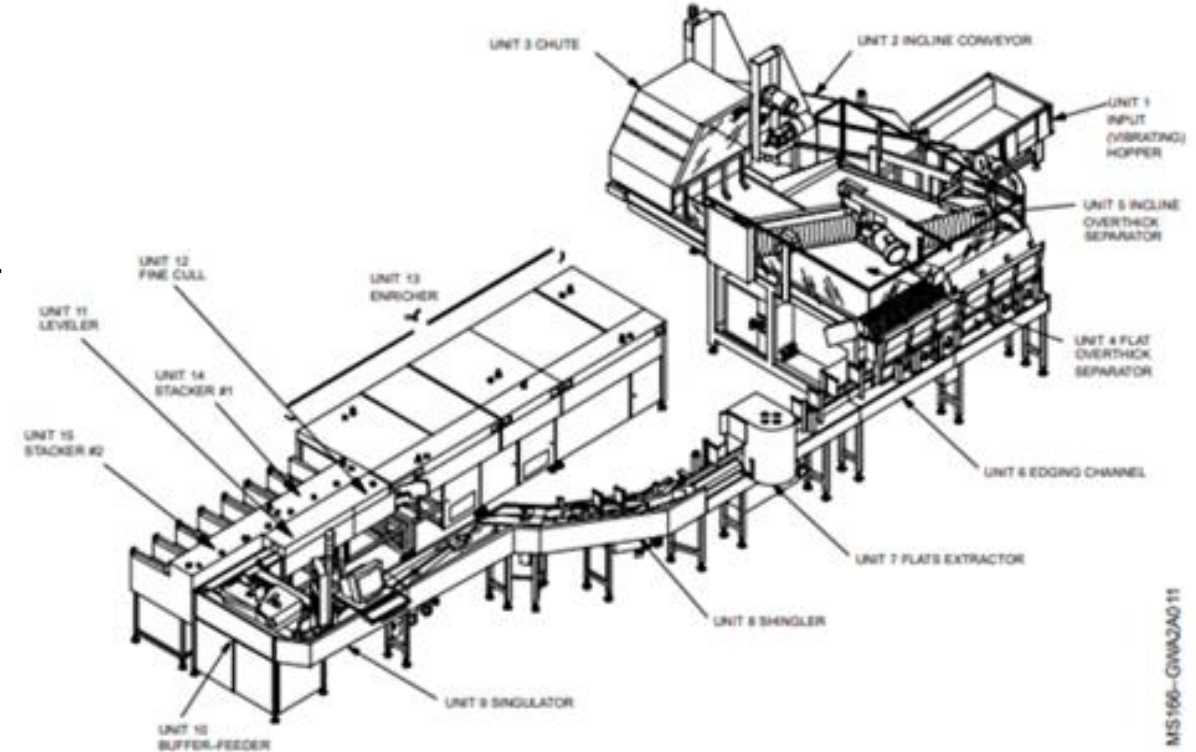
					
					
					
					
					
					
					

## Countermeasures



# Advanced Facer Cancellation System (AFCS)

- High-speed machine used by the US Postal Service to cull, face, and cancel letter mail through a series of automated operations.
- Capable of processing 30,000 pieces of mail per hour.
- Downtime is escalated if after 10 minutes
- Pre-program boards control movement of parcels
- **Sabotage Example:**  
Time based attack programmed into PLC board



The Culler Section consists of the following units:

- a. Unit 1, Input Hopper
- b. Unit 2, Incline Conveyor
- c. Unit 3, Chute
- d. Unit 4, Overthick Separator Flat
- e. Unit 5, Overthick Separator Incline
- f. Unit 6, Edging Channel
- g. Unit 7, Flats Extractor
- h. Unit 8, Shingler
- i. Unit 9, Singulator
- j. Unit 10, Buffer/Feeder





# Delivery Bar Mail Sorters (DBMS)

Prepare incoming and outgoing **mail** for distribution. Examine, sort, and route **mail**.

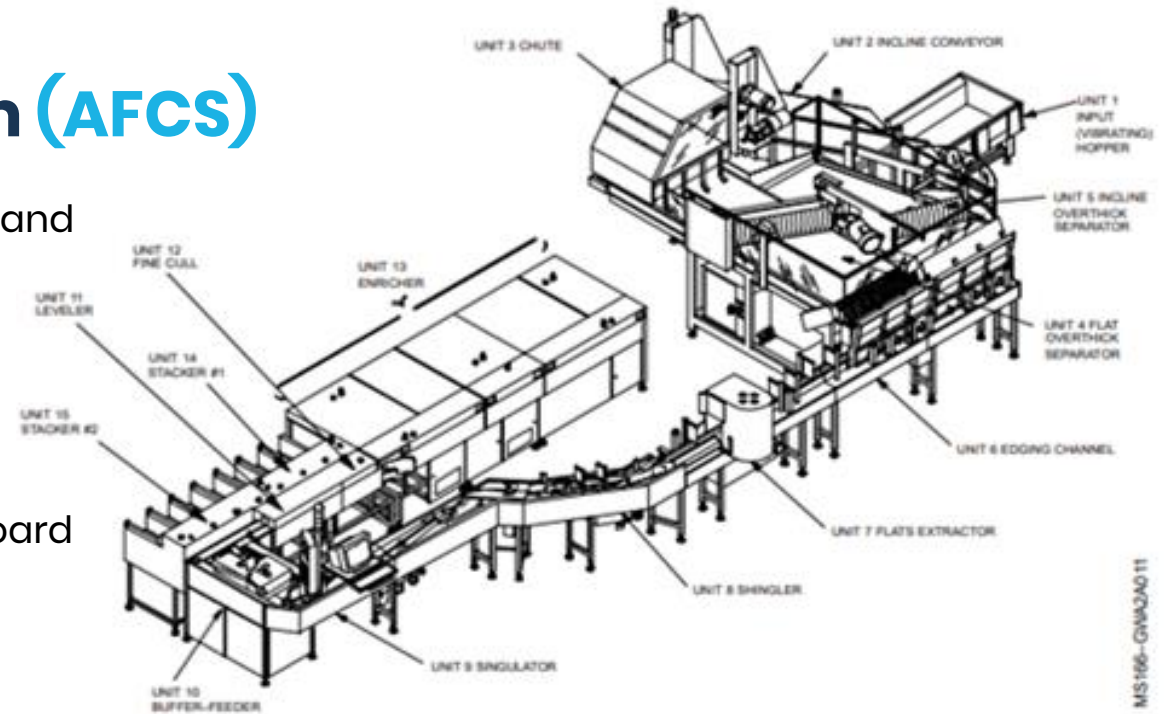
Load, operate, and occasionally adjust and repair **mail** processing, sorting, and canceling machinery.

Keep records of shipments, pouches, and sacks; and other **duties** related to **mail** handling within the **postal** service.



## Advanced Facer Cancellation System (AFCS)

- High-speed machine used by the US Postal Service to cull, face, and cancel letter mail through a series of automated operations.
- Capable of processing 30,000 pieces of mail per hour.
- Downtime is escalated if after 10 minutes
- Pre-program boards control movement of parcels
- Sabotage Example: Time based attack programmed into PLC board



MS166-GW02AO11

The Culler Section consists of the following units:

- Unit 1, Input Hopper
- Unit 2, Incline Conveyor
- Unit 3, Chute
- Unit 4, Overthick Separator Flat
- Unit 5, Overthick Separator Incline
- Unit 6, Edging Channel
- Unit 7, Flats Extractor
- Unit 8, Shingler
- Unit 9, Singulator
- Unit 10, Buffer/Feeder

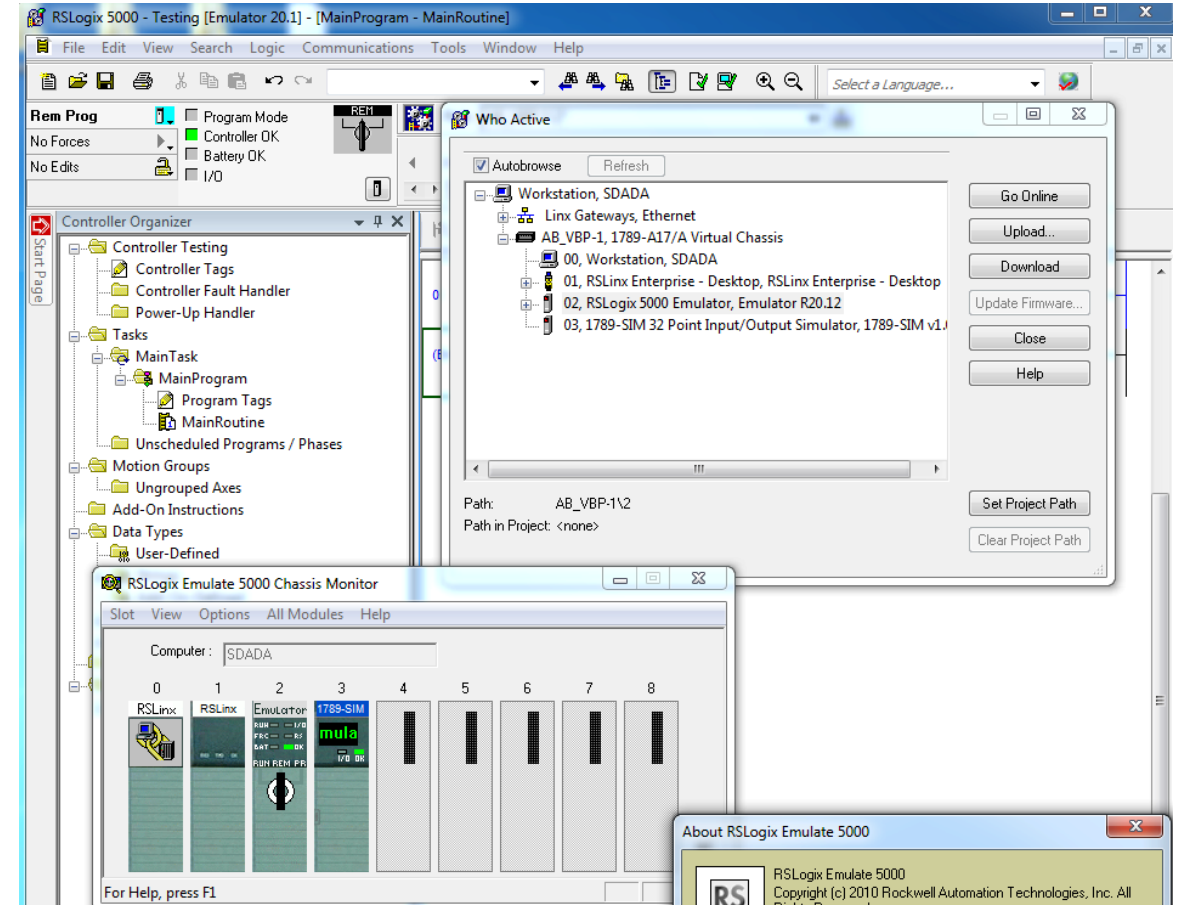


# Code, Package, Infiltrate



Target components (example):

- RSLogix 5000
  - RSView Studio
  - Drive Executive
  - RSNetWorx
  - RSSql
- 
- Response usually means swapping out PLC component
  - Advanced attack pattern would be to make code persistent to local filesystem where privileges are inherited.
  - Most binary files are not signed in similar environments; no assurance
  - Open Trust Boundaries to other Callers or storage components

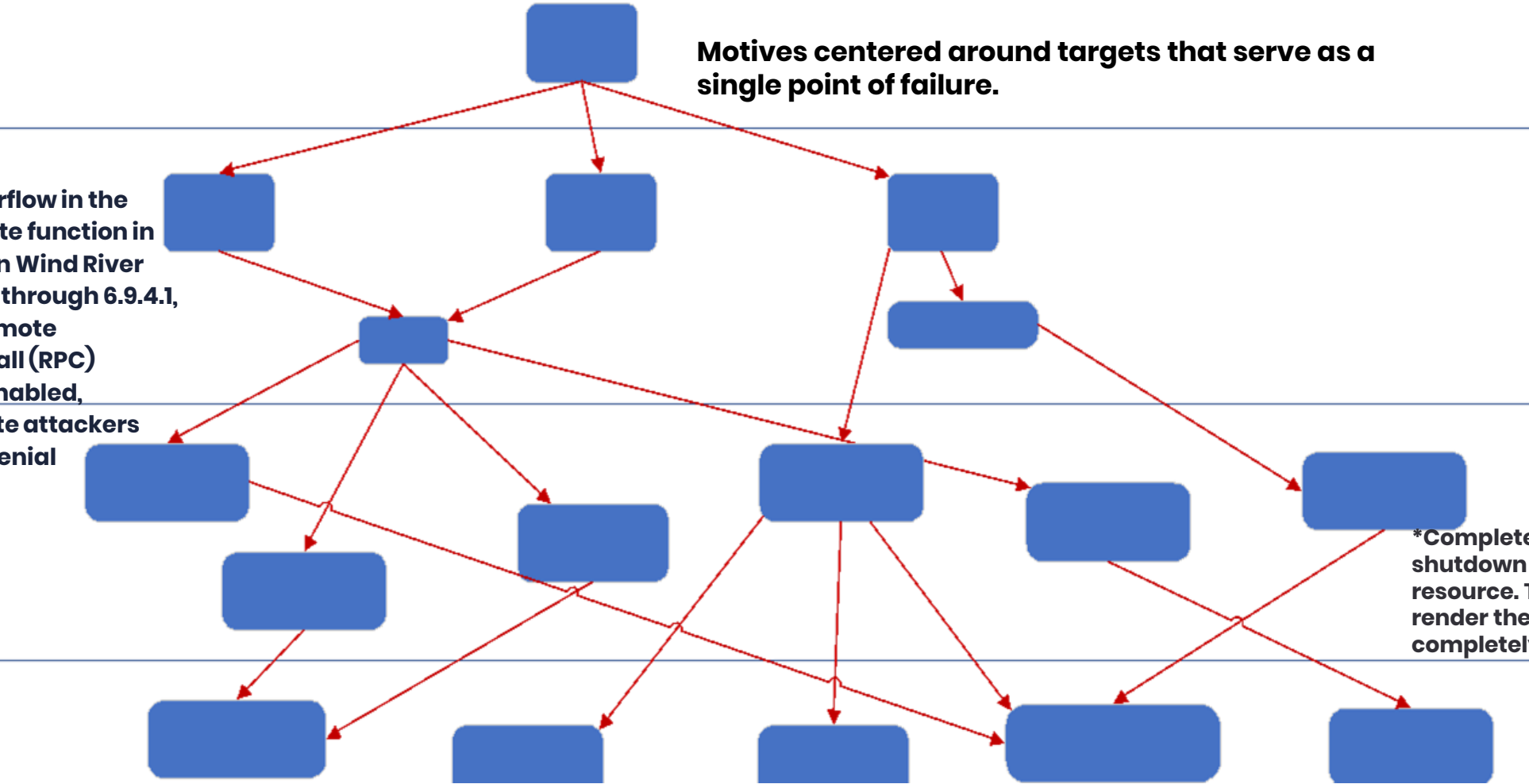


# Threat of Sabotage – Attack Tree Example



\*Integer overflow in the `_authenticate` function in `svc_auth.c` in Wind River VxWorks 5.5 through 6.9.4.1, when the Remote Procedure Call (RPC) protocol is enabled, allows remote attackers to cause a denial of service.

Motives centered around targets that serve as a single point of failure.



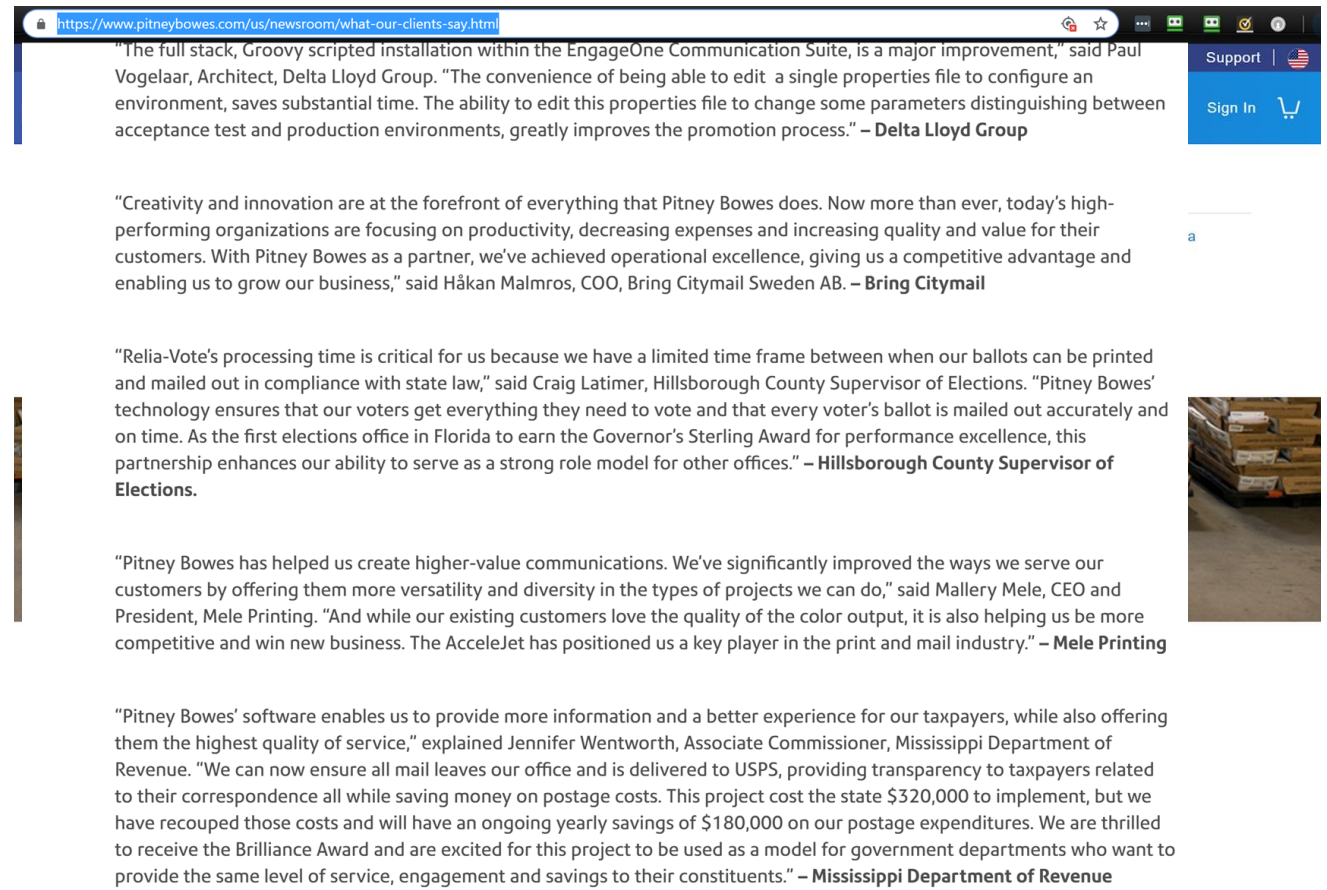
\*Complete (There is a total shutdown of the affected resource. The attacker can render the resource completely unavailable.)

# Supply Chain Target Selection

## Select Objective

- Steal data
- Persist in target environment
- IP Theft for overseas competitor
- Sabotage
- Extort
- Chaining objectives for more intricate attack plans

## Target Selection



<https://www.pitneybowes.com/us/newsroom/what-our-clients-say.html>

"The full stack, Groovy scripted installation within the EngageOne Communication Suite, is a major improvement," said Paul Vogelaar, Architect, Delta Lloyd Group. "The convenience of being able to edit a single properties file to configure an environment, saves substantial time. The ability to edit this properties file to change some parameters distinguishing between acceptance test and production environments, greatly improves the promotion process." – **Delta Lloyd Group**

"Creativity and innovation are at the forefront of everything that Pitney Bowes does. Now more than ever, today's high-performing organizations are focusing on productivity, decreasing expenses and increasing quality and value for their customers. With Pitney Bowes as a partner, we've achieved operational excellence, giving us a competitive advantage and enabling us to grow our business," said Håkan Malmros, COO, Bring Citymail Sweden AB. – **Bring Citymail**

"Relia-Vote's processing time is critical for us because we have a limited time frame between when our ballots can be printed and mailed out in compliance with state law," said Craig Latimer, Hillsborough County Supervisor of Elections. "Pitney Bowes' technology ensures that our voters get everything they need to vote and that every voter's ballot is mailed out accurately and on time. As the first elections office in Florida to earn the Governor's Sterling Award for performance excellence, this partnership enhances our ability to serve as a strong role model for other offices." – **Hillsborough County Supervisor of Elections**

"Pitney Bowes has helped us create higher-value communications. We've significantly improved the ways we serve our customers by offering them more versatility and diversity in the types of projects we can do," said Mallery Mele, CEO and President, Mele Printing. "And while our existing customers love the quality of the color output, it is also helping us be more competitive and win new business. The AcceleJet has positioned us a key player in the print and mail industry." – **Mele Printing**

"Pitney Bowes' software enables us to provide more information and a better experience for our taxpayers, while also offering them the highest quality of service," explained Jennifer Wentworth, Associate Commissioner, Mississippi Department of Revenue. "We can now ensure all mail leaves our office and is delivered to USPS, providing transparency to taxpayers related to their correspondence all while saving money on postage costs. This project cost the state \$320,000 to implement, but we have recouped those costs and will have an ongoing yearly savings of \$180,000 on our postage expenditures. We are thrilled to receive the Brilliance Award and are excited for this project to be used as a model for government departments who want to provide the same level of service, engagement and savings to their constituents." – **Mississippi Department of Revenue**

# Supply Chain Target Selection



## Select Objective

Steal data

Persist in target environment

IP Theft for overseas competitor

Sabotage

Extort

Chaining objectives for more

intricate attack plans

## Target Selection

The screenshot shows a web browser window with the URL <https://www.pitneybowes.com/us/newsroom/what-our-clients-say.html>. The page features several testimonials from clients. The first testimonial is from Paul Vogelaar, Architect at Delta Lloyd Group, praising the EngageOne Communication Suite. The second is from Håkan Malmros, COO at Bring Citymail, highlighting Pitney Bowes' creativity and innovation. The third is from Craig Latimer, Hillsborough County Supervisor of Elections, noting the company's reliability and compliance. The fourth is from Mallery Mele, CEO at Mele Printing, appreciating the company's versatility and quality. The fifth is from Jennifer Wentworth, Associate Commissioner at the Mississippi Department of Revenue, praising the company's software and service quality.

"The full stack, Groovy scripted installation within the EngageOne Communication Suite, is a major improvement," said Paul Vogelaar, Architect, Delta Lloyd Group. "The convenience of being able to edit a single properties file to configure an environment, saves substantial time. The ability to edit this properties file to change some parameters distinguishing between acceptance test and production environments, greatly improves the promotion process." – **Delta Lloyd Group**

"Creativity and innovation are at the forefront of everything that Pitney Bowes does. Now more than ever, today's high-performing organizations are focusing on productivity, decreasing expenses and increasing quality and value for their customers. With Pitney Bowes as a partner, we've achieved operational excellence, giving us a competitive advantage and enabling us to grow our business," said Håkan Malmros, COO, Bring Citymail Sweden AB. – **Bring Citymail**

"Relia-Vote's processing time is critical for us because we have a limited time frame between when our ballots can be printed and mailed out in compliance with state law," said Craig Latimer, Hillsborough County Supervisor of Elections. "Pitney Bowes' technology ensures that our voters get everything they need to vote and that every voter's ballot is mailed out accurately and on time. As the first elections office in Florida to earn the Governor's Sterling Award for performance excellence, this partnership enhances our ability to serve as a strong role model for other offices." – **Hillsborough County Supervisor of Elections.**

"Pitney Bowes has helped us create higher-value communications. We've significantly improved the ways we serve our customers by offering them more versatility and diversity in the types of projects we can do," said Mallery Mele, CEO and President, Mele Printing. "And while our existing customers love the quality of the color output, it is also helping us be more competitive and win new business. The AcceleJet has positioned us a key player in the print and mail industry." – **Mele Printing**

"Pitney Bowes' software enables us to provide more information and a better experience for our taxpayers, while also offering them the highest quality of service," explained Jennifer Wentworth, Associate Commissioner, Mississippi Department of Revenue. "We can now ensure all mail leaves our office and is delivered to USPS, providing transparency to taxpayers related to their correspondence all while saving money on postage costs. This project cost the state \$320,000 to implement, but we have recouped those costs and will have an ongoing yearly savings of \$180,000 on our postage expenditures. We are thrilled to receive the Brilliance Award and are excited for this project to be used as a model for government departments who want to provide the same level of service, engagement and savings to their constituents." – **Mississippi Department of Revenue**

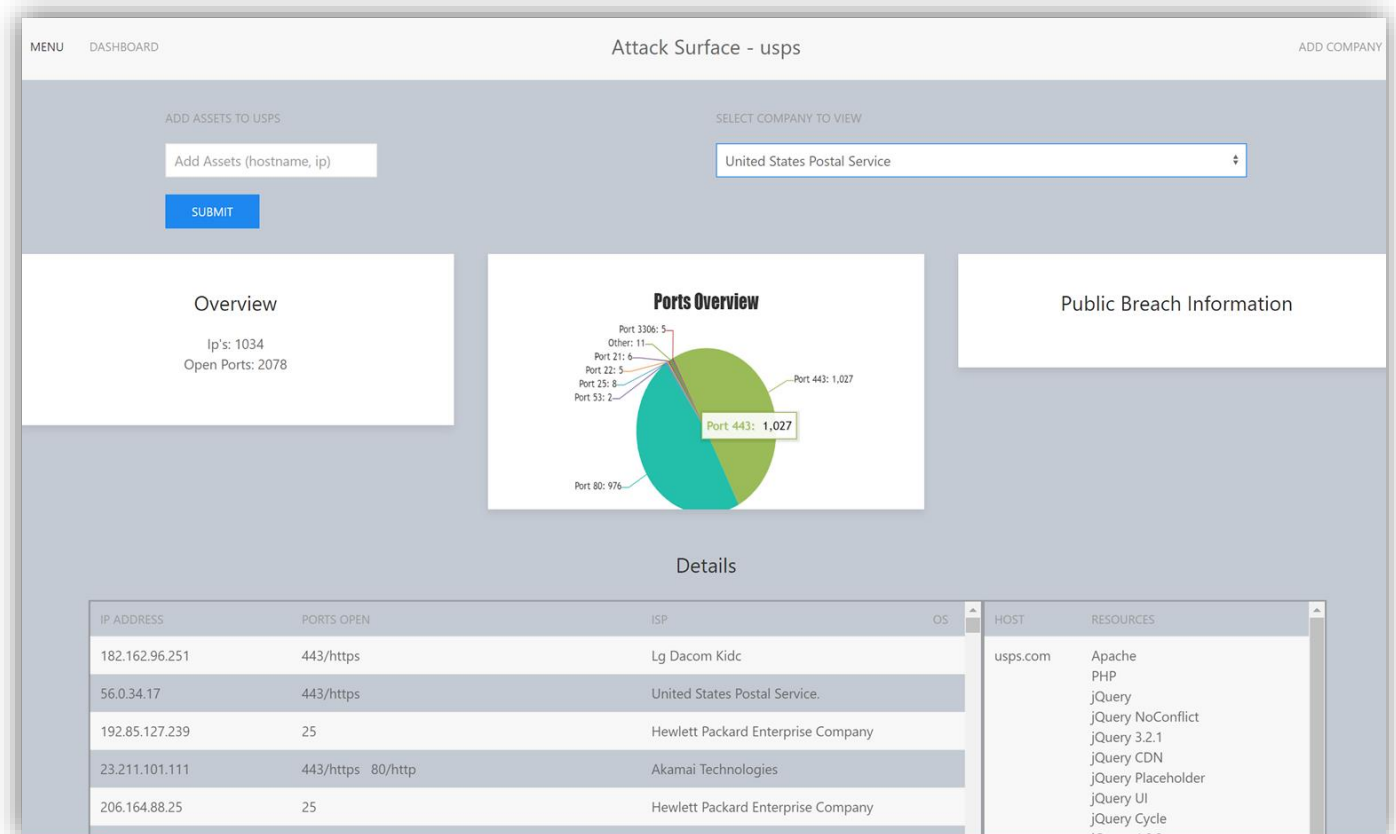


# Defining Intended Attack Surface

## Select Objective

- APIs
- HW components w/ PLC
- Environments rich for collusion
- Human operators as targets
- Components that support Create-Read-Update-Delete rights needed
- Components w/ write access to storage locations

## Vigilance on Target Assets

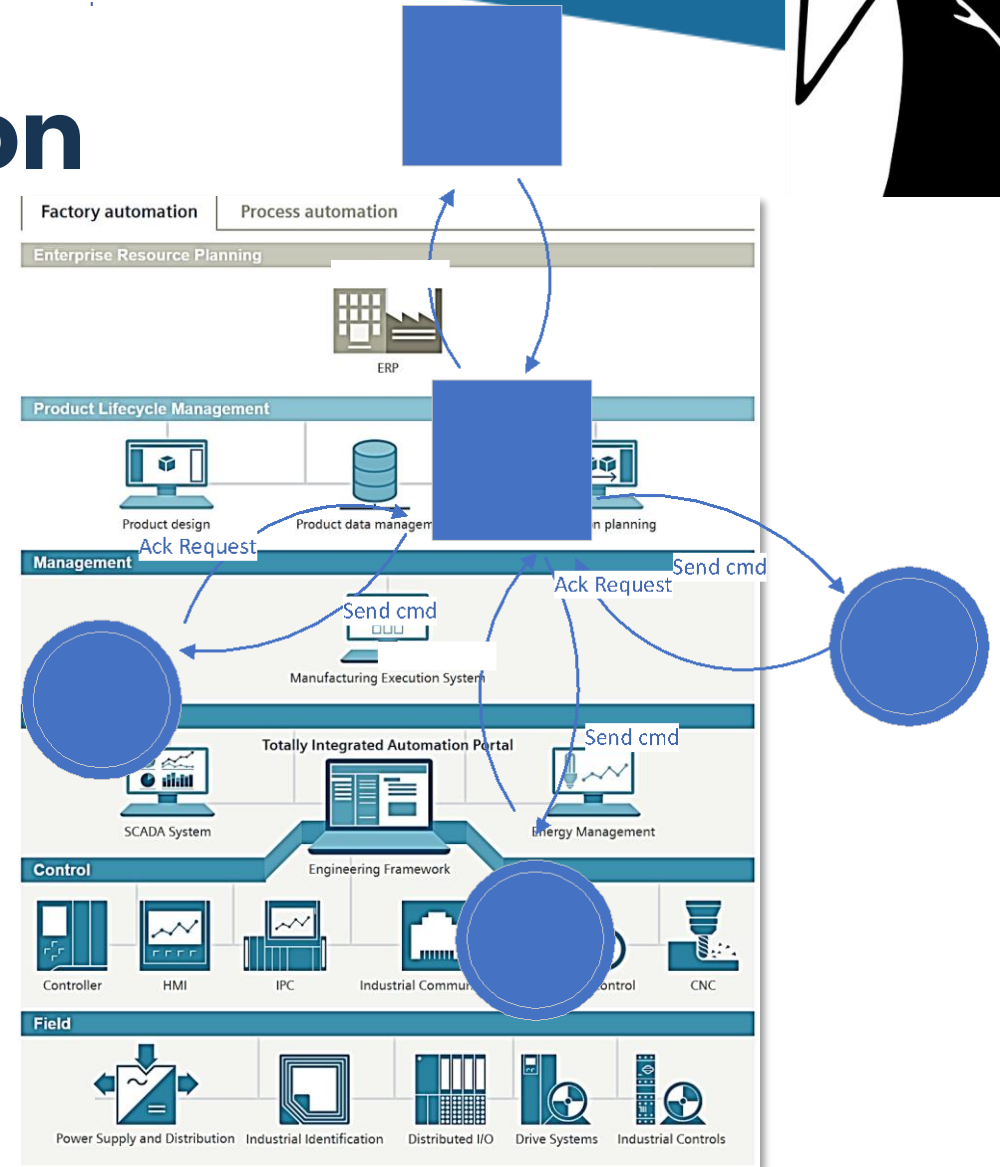




# Abusing Trust in Automation

## Exploiting Weak System/ Component Architecture

- Implicit system trust models
- No request inspection
- No cert validation to compiled code objects
- No code inspection
- No security assurance in product/ code upstream



# Sustaining Threats

- Personal data continues to be an inherent threat for sources of PII
- Probabilistic analysis can be done on events at USPS

$$\text{PROBABILITY} = \frac{\text{EVENT}}{\text{OUTCOMES}}$$

- For other unrealized threats would required predictive analysis
- Sabotage (realized)
- Extortion (unrealized)
- Cryptomining (unrealized)

## 21 USPS Site Exposed Data on 60 Million Users

NOV 18

**U.S. Postal Service** just fixed a security weakness that allowed anyone who has an account at **usps.com** to view account details for some 60 million other users, and in some cases to modify account details on their behalf.

## 2 USPS 'Informed Delivery' Is Stalker's Dream

OCT 17

A free new service from the **U.S. Postal Service** that provides scanned images of incoming mail before it is slated to arrive at its destination address is raising eyebrows among security experts who worry about the service's potential for misuse by private investigators, identity thieves, stalkers or abusive ex-partners. The **USPS** says it hopes to have changes in place by early next year that could help blunt some of those concerns.

The service, dubbed "**Informed Delivery**," has been available to select addresses in several states since 2014 under a targeted **USPS** pilot program, but it has since expanded to include many ZIP codes nationwide, according to the Postal Service. U.S. residents can tell if their address is eligible by visiting [informedelivery.usps.com](http://informedelivery.usps.com).



m

researcher who discovered the problem, but said he informed the USPS about his findings. After confirming his findings, the USPS addressed the issue.

The weakness in a USPS Web component known as "Informed Delivery," a set of tools defining how various identified Web pages should interact with one

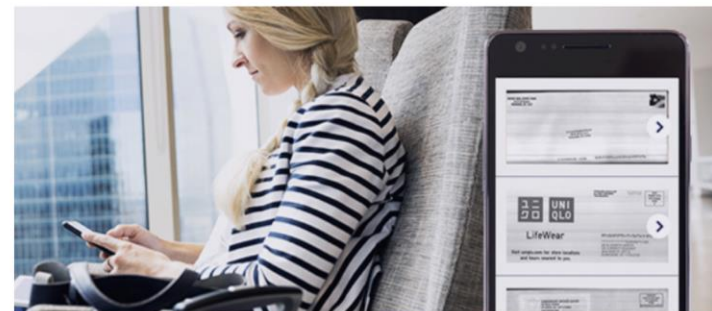


Image: USPS

# Blueprint for Vuln Identification & Attacks

## (Prescriptive Guidance)



- Wrap exploitation testing into your threat model
- Identify the attack surface that causes intended impact (PASTA Stage II)
- Build attack patterns to exercise from threat library developed (PASTA Stage IV)
- Correlate identified vulns to attack surface (PASTA – Stage V)
- Identify branches of attack that fulfill threat objectives & exploit identified vulns (PASTA – Stage VI)
- Conduct exploit testing on these abuse cases to identify viability and factor into probabilistic analysis (PASTA – Stage VII)
- 0-Day development against target components that fulfill threat objectives (PASTA – Stage VI)





# Blueprint for Mitigation

## Prescriptive Guidance

- Identify the attack surface that causes intended **impact** (PASTA Stage II)
- Review what **regulatory** requirements affect processes or technology components within the scope of your threat model (PASTA Stage II)
- **Pre-emptively** considers regulations in system/ solution design
- **Inspect & harden** controls that reduce attack vectors or vulns (PASTA – Stage II)
- Understand where the **logical** and **physical trust boundaries** exist for your attack surface (PASTA – STAGE III)
- Consider **probability values** for attack patterns to be successful based upon prevalence of threat intel & data + CVSS (PASTA – Stage VII)
- Determine residual risk per **attack pattern** that is tested against **associated vulns**, and that correlates to **current threat data/ threat advisories**

# Final Thoughts





**VERSPRITE**

“Software- and hardware-based supply chain attacks are also trending up... Consequently, ***monitoring higher layers for behavior indicative of an attack*** is crucial to obtain better protection against advanced adversaries.”

**- Gartner June 2018**

# Risks Escalating & Changing

- 2017 saw a dramatic rise in supply chain attacks, over the previous years- 200% increase
- Typical attacks costs a business \$1.1 million
- While physical attackers can hijack a truck, harm a driver, and steal cargo, attacks on payment pages, a company's IT provider, etc, can lead to much longer-term attacks that may siphon off much more money before they are discovered
- Amazon going down costs ~ \$230,000+ per minute
- More executives report planning to be more directly involved in the planning, detection, and response to such incidents



## Process for Attack Simulation & Threat Analysis (PASTA)



# Offensive Intel to Consider

The following is currently is being carried out:

- Similar to aggregating compromised PII into a marketplace, a marketplace for companies vulns and attack surface exists
- Attack Surface profiles for target entities
- Government groups, private hacker syndicates for hire most mature in this area

Attack Surface is a living information source

- Re-calibrating attack surface

Map Threat Objective to Attack Surface

- Steal IP: Identify IP sources from public private repos via logical & human based attacks
- Extort: Identify mission critical systems / data sources that have weak redundancy/ failover capabilities
- Framing: Create attack pattern with 'signatures' of known adversary to target for diversion attacks
- Cyberwar: Disrupt critical infrastructure that impedes delivery, social services, communication
- Map attack service components to above and maintain DB of vulns associated w/ component nodes

**IT'S OK YOU GOT  
TRAINING WHEELS**



## Threat Modeling Supply Chain Environments with STRIDE

- Threat models necessitate accurate threat libs
- STRIDE doesn't factor in any threat intel/ data
- Threat modelers can't be limited by 6 constant threat classes
- Organizing threats less important than substantiating them
- Threats, motives, threat actors are unique to industry, business





# Whitehat Guidance to Supply Chain Threat Models

## Prescriptive Guidance

- Leverage a Risk Based approach to threat modeling to blueprint adversarial exercises and simulations
- Qualify Threats and incorporate into your model
- Substantiate threats with intel and threat data
- Where are you weakest against a threat lib for supply chain?
- Architecture & Physical Security (low hanging fruit)
- Recommend onboarding teams include you to supplier meetings in order to address security assurance
- Assess your logical risks for over the network-based attacks
- Feed log repos with log events that monitor attack or recon patterns from supply chain threat model
- Manage open risks with broader team
- Don't be a security sheep - no one knows your business, industry better than you. Build your own threat library





# Tony UcedaVélez

CEO & Founder, VerSprite

**VerSprite.com – Global Security Firm**

- OWASP Atlanta Chapter Leader (past 10 years)
- Author, *“Risk Centric Threat Modeling – Process for Attack Simulation & Threat Analysis,”* Wiley June 2015
- Passionate global, threat modeling evangelist
- Dreams of bankrupting #infosec with intelligent, threat inspired DevSecOps automation

