



2025 Cybersecurity Landscape for Manufacturers:

Risks, Threats, and Best Practices

SPEAKER



Christopher Fielder

FIELD CTO, ARCTIC WOLF



AGENDA

- 01** Factors contributing to the rise of manufacturing breaches
- 02** Who is attacking manufacturers
- 03** What are they doing
- 04** How are they doing it
- 05** Best practices



Poll Question 1



Manufacturers have become the most targeted vertical

2023

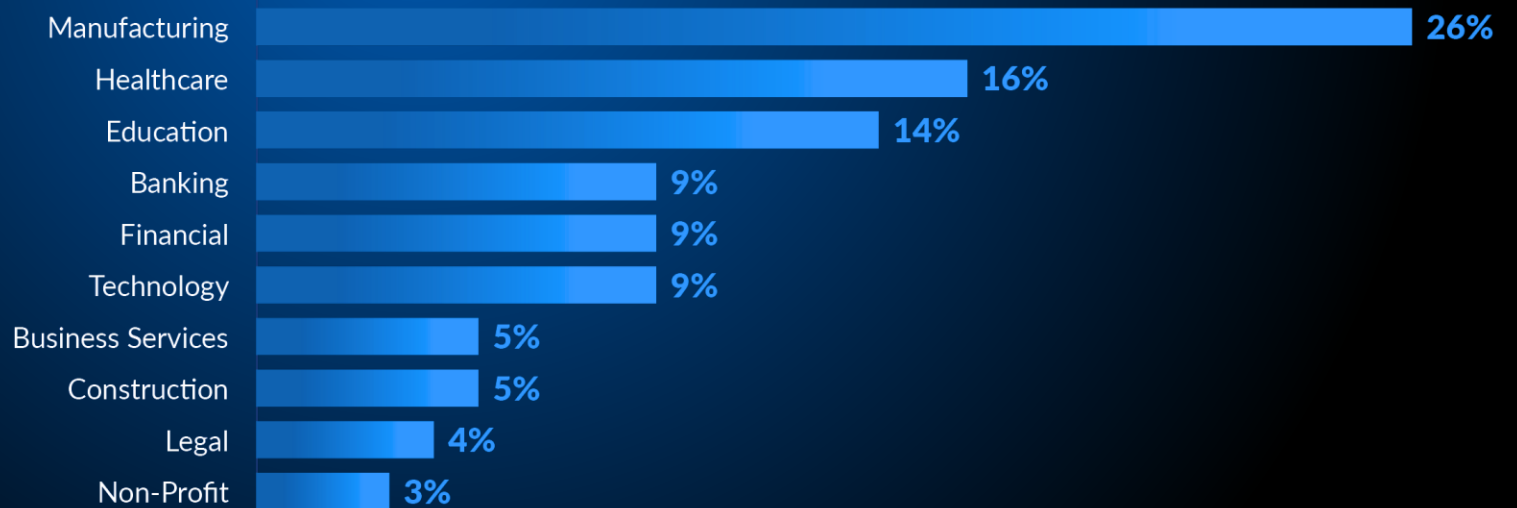
Manufacturing was the 3rd most targeted vertical worldwide

Determined by a normalized calculation of alerts generated, confirmed breaches, and incident response cases

2024

Manufacturing is now the #1 most targeted vertical

- By a vast margin (in some areas by as much as a 2.6X ratio) across 20+ verticals
- Manufacturing is #1 in alerts generated and confirmed threats detected
- Manufacturing is #1 most engaged vertical for Incident Response cases



Manufacturers Beware

Factors contributing to the rise of breaches

- 1 Legacy perimeter threats leveraged against a "perimeter-less" world
- 2 Targeting from nation-state actors that want to be leaders in manufacturing
- 3 Manufacturing is at the root/foundation of the supply chain
 - Collateral damage associated with the final target
 - Willingness to negotiate centered around the need for "zero downtime"

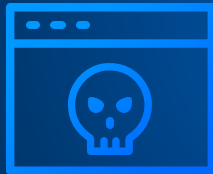


You Are All Aware of the Problem

Let's discuss the important details



Who are the
Threat Actors



What are
they doing?



How are they
accomplishing
their goals?



How do we prepare
or prevent these
situations?




Who?



Threat Actors

The Usual Suspects, Defined



**NATION-STATE
SPONSORED
ACTOR**

MOTIVATORS

- Political

TECHNIQUES

- Zero-day vulnerabilities
- Hidden Malware



**RANSOMWARE
AS A SERVICE OPERATORS**

MOTIVATORS

- Financial Motivation

TECHNIQUES

- Ransomware

Threat Actors

Key players in manufacturing

Nation States

China
Iran
Russia
North Korea

DRIVERS

Espionage, Political
Influence, Data Theft,
Destruction

Ransomware "Gangs"

Akira
Play
Black Basta
Lockbit

DRIVERS

Financial Gain,
Data Theft

BEC Groups

Individual Threat Actors
Loose Associations
Opportunistic "watering
holes"
Less Sophisticated

DRIVERS

Financial Gain,
Data Theft,
Social Engineering

Hacktivists

CyberVolk
Z-Pentest
Anonymous
(questionable)

DRIVERS

Political Activism,
Retaliation, Advocacy



Top 4 most active Threat Actors

From our data

LOCKBIT

- 775 Victims in 12-month period
- Manufacturing was 20% of their victims
- Averages 65 posts per month on leak site
- Median starting demand \$1M USD

PLAY

- 386 victims in 12 months
- Manufacturing was 19%, Construction 18% of their victims
- Averages 32 posts per month on leak site
- Median starting demand \$5.6M USD

AKIRA

- 215 victims in 12 months,
- Manufacturing was 23% of their victims
- Averages 19 posts per month on their leak site
- Median starting demand \$325,000 USD

BLACK SUIT

- 116 Victims in 12 months
- Manufacturing was 15% of their victims
- Averages 10 posts per month on leak site
- Median starting demand \$650,000 USD



What?



Top 3 manufacturing incident types in 2024

Threat Actor Goals



58%*

**Ransomware and Data
Extortion**



23%

**Business Email
Compromise**



19%

**Network or
Host Intrusion**

*44% across all verticals, a 14% increase in manufacturing specifically

© 2025 Arctic Wolf Networks, Inc. All rights reserved. Public



The high cost of ransomware

96% of ransomware incidents included data exfiltration*

94% of those who suffered a ransom event experienced a period of significant downtime and delays in productivity**

50% of ransomware victims reported productivity impacts of four months to a year following the attack**

*Arctic Wolf 2025 Threat Report

**The State of Cybersecurity: 2024 Trends Report

© 2025 Arctic Wolf Networks, Inc. All rights reserved. Public

Organizations with \$500M+ Annual Revenues

WELL-KNOWN COSTS:

- Forensics
- Incident Response Legal Counsel
- Restoration & Recovery
- Notifications to Customers and Vendor Costs
- PR Costs
- Regulatory Fines

\$1.1M

LESSER-KNOWN COSTS:

- Ransom Payment
- Lawsuits
- Data Mining
- Credit Monitoring

\$10.2M

WHERE INSURANCE COVERAGE (TYPICALLY) ENDS

\$18.8M

Revenue
Downtime

22 days of lost profits¹

\$3.4M

Wasted
Payroll

50% of employees not
producing for 22 days

\$7.8M

Loss of Future
Revenues

10% drop in profits from
lost revenues for the
following 3 months^{2,4}

\$54M

Company Valuation
Decline

3% lower stock price after
6 months^{3,4}

BEC Stats

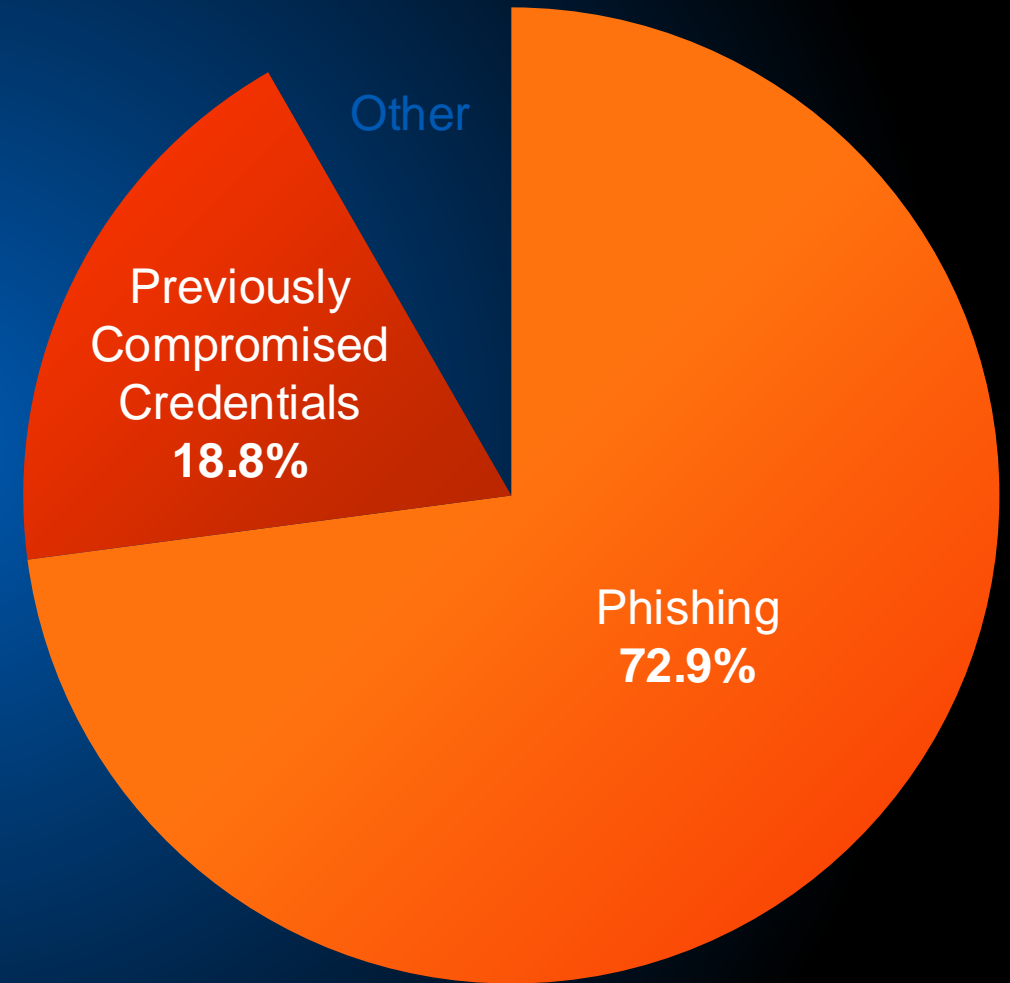
BEC incidents are the second-largest cause of IR cases:

Business email compromise was the primary impacting factor in 27% of our IR incidents

Phishing awareness and access controls are strong preventative measures:

Phishing (72.9%) and **previously compromised credentials (18.8%)** are the leading root causes of BEC cases, pointing to employee training, credential management, and biometric or possession-based MFA as effective defenses.

*Arctic Wolf 2025 Threat Report



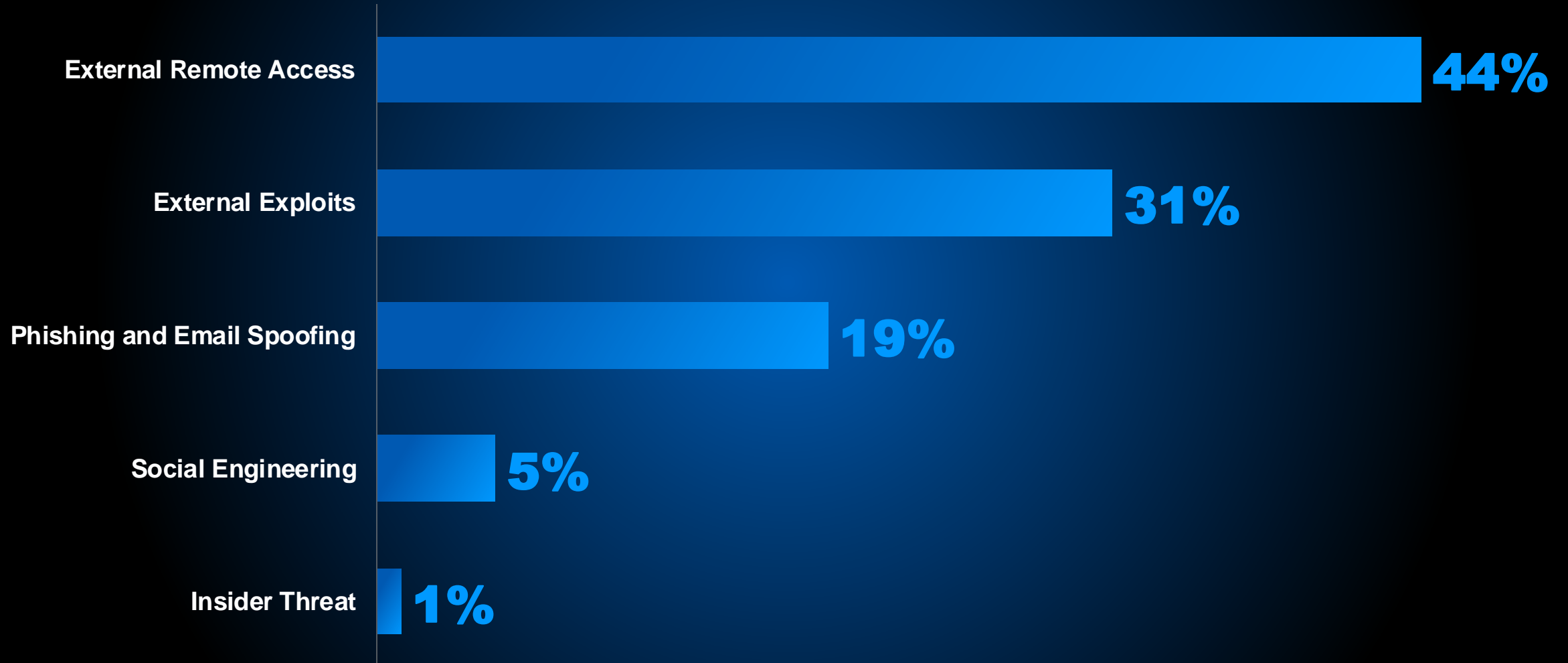
How?



Poll Question 2



Top 5 RPOCs in Manufacturing 2024



**Manufacturing leads all industry
verticals in External Remote Access
and External Exploits used as RPOC**



Best Practices

Safeguarding your business



Secure remote access

- Enforce MFA and change default passwords!
- Limit access through segmentation and least privilege
- Monitor these tools 24/7 and update/patch regularly



Limiting effectiveness of external exploits

- Implement robust & redundant patch management process
- Minimize attack surface with network hardening
- Leverage threat detection and prevention technology



Poll Question 3



Thank You



Contact Us

Our cybersecurity experts are ready to help.

REQUEST A DEMO

ADDRESS

8939 Columbine Rd
Eden Prairie, MN 55347

CONTACT

arcticwolf.com
1-888-272-8429

SOCIAL



OT and Automation

Manufacturing networks are made up of a range of devices, including OT (smart) devices and specialized network devices

**“Secure the path to OT
rather than OT itself”**

