In partnership with Cyentia Institute

Anatomy of 100+ Cybersecurity Incidents in Industrial Operations:

A Research Study With Recommendations For Strengthening Defenses in OT/ICS

Sponsored by

Rockwell Automation

Table of Contents

Preview of things to come

In 1982, a Trojan program was inserted into supervisory control and data acquisition (SCADA) system software controlling the USSR's Siberian natural gas pipeline, which caused a massive natural gas explosion along the Trans-Siberian pipeline. A KGB insider revealed a specific shopping list and the CIA slipped the flawed software to the Soviets in a way they would not detect it. The objective was to disrupt the Soviet gas supply, its hard currency earnings from the West, and the internal Russian economy. The pipeline software that was to run the pumps, turbines, and valves was programmed to go haywire after a decent interval, to reset pump speeds and valve settings to produce pressures far beyond those acceptable to pipeline joints and welds.

The result was the most monumental non-nuclear explosion and fire ever seen from space.

Sources:
Thomas C. Reed, former secretary of the Air Force and special assistant to President Reagan, At the Abyss: An Insider's History of the Cold War.
Additional news source: https://www.wired.com/2004/03/soviets-burned-by-cia-hackers/

Introduction & Research Methodology

Understanding Industrial Cyberattack Patterns

In an increasingly interconnected world, our reliance on opertational technology (OT) systems has exponentially expanded. These industrial systems underpin essential infrastructure, manufacturing processes, and transportation networks.

At the same time, these systems are vulnerable to cyberthreats that can have devastating consequences. And, as OT/integrated control systems (ICS) are integrated into enterprise IT networks, the line between digital and physical infrastructure continues to blur. Whether your organization makes cookies or cars, you're constantly adding assets to the network, which only expands an already dynamic attack surface.

Having a framework to accommodate all changes and virtual assets on modern networks, and protecting everything physical and virtual — while still maintaining OT operations at a very high level of availability — are big challenges organizations face today.

This report lays out the results of an in-depth historical research study into the anatomy of OT cybersecurity incidents.

Our research sample was tightly focused on OT/ICS security incidents. In total, we analyzed 122 OT incidents spread across five continents, including North America, Europe, the Middle East, Asia and Africa.

We recognize that the cybersecurity protection challenges aren't limited to industrial operations alone. Gartner predicts that by 2025, 45% of global organizations will have experienced attacks on their software supply chains, a three-fold increase from 2021. The Identity Theft Resource Center recently reported that U.S. organizations issued 1,802 data breach notifications, affecting more than 400 million individuals in 2022.[1]

Due to the complex technological infrastructures in place, the industrial sector is traditionally slower to adopt new processes and tools. This is why we wanted to share insights into strategies and tactics found in other OT cybersecurity incidents to underscore the importance of proactively protecting OT operations.

Rockwell Automation commissioned the Cyentia Institute to analyze cybersecurity events involving compromised OT/ICS. Cyentia, an analyst firm specializing in cybersecurity research, reviewed the subject data set and built several models to examine relationships around the data, revealing patterns that led to the conclusions in this report. The data set used by Cyentia for this analysis is from Advisen's global, proprietary Cybersecurity Loss Database.

This is considered the largest global database of publicly-known security incidents. Each incident in the database may include up to 1,000 individual data points. The data is used heavily by commercial property and casualty insurers to provide insights for corporate risk profiles, and to inform strategic business decisions, including as inputs to setting cybersecurity insurance rates and terms.

From an initial sampling of public and private incidents meeting target criteria from the Advisen Cybersecurity Loss Database, Cyentia performed further research on each incident using multiple sources of public information, collecting nearly 100 data points for each incident. To increase relevance, if the analysis determined that an event did not involve the direct compromise of OT/ICS, disrupt or negatively impact OT/ICS operations, or expose sensitive information on OT/ICS operations, we excluded that incident from our data set for this study.

In all, we removed 25 events that did not meet the aforementioned criteria. This left 122 events, from 1982 through 2022. These formed the representative sampling of OT/ICS compromise events analyzed in this study.

Rockwell Automation's goal

This study was commissioned to develop and share instructive insights around actual OT/ICS cybersecurity attack activity. We know it's imperative to prioritize the protection of OT systems, invest in advanced cybersecurity technologies, and raise awareness among industrial leaders These insights should help defenders better understand the true nature of the battleground they face, and support taking more urgent action to improve defenses.

Source[1]: 2022 Data Breach Report

Primary Research Findings

Primary findings include:

Critical Infrastructure faces rising risks

Critical Infrastructure vertical industries appear in the top five most targeted industries, with several more in the top 10.

Intensely focused on energy

Attacks are most intensely focused on energy sectors – 3X more than the next most frequently attacked vertical.

Aiming to disrupt

Most attacks on OT/ICS systems aim to disrupt operations using a variety of tools and techniques, from phishing to ransomware to lateral tool transfer and exploitation of remote services.

Attackers gaining access to IT networks

Attackers are gaining access to IT networks first in most OT incidents.

Nation-state sponsored

Many attacks were found to be nation-state sponsored, indirectly enabled by internal personnel about one-third of the time.

Phishing

Phishing is the most popular attack technique.

Key Findings

OT/ICS security incidents are increasing in frequency every year.

- Just a few years into the most recent decade, and we have already exceeded the number of incidents reported in the decade running from 1991-2000.
- In 2022, industry reports indicated a 2,000% increase in adversarial reconnaissance targeting Modbus/TCP port 502, a commonly used industrial protocol, which could allow hackers to control physical devices and disrupt OT operations.[2]
- Event frequency data is likely to increase not only due to targeting, but also because there are better detection tools and capabilities available to help identify cybersecurity incidents.
- Figure 1 highlights the total number of incidents analyzed (122). Other percentage charts in this report may exceed 100% because options analyzed are not mutually exclusive. Many incidents involve multiple, simultaneous characteristics, and each is independently analyzed, which is why total percentages may exceed 100%. This type of analysis underscores the complex nature of cybersecurity incidents and the various factors contributing to them.

Rockwell Automation finds:

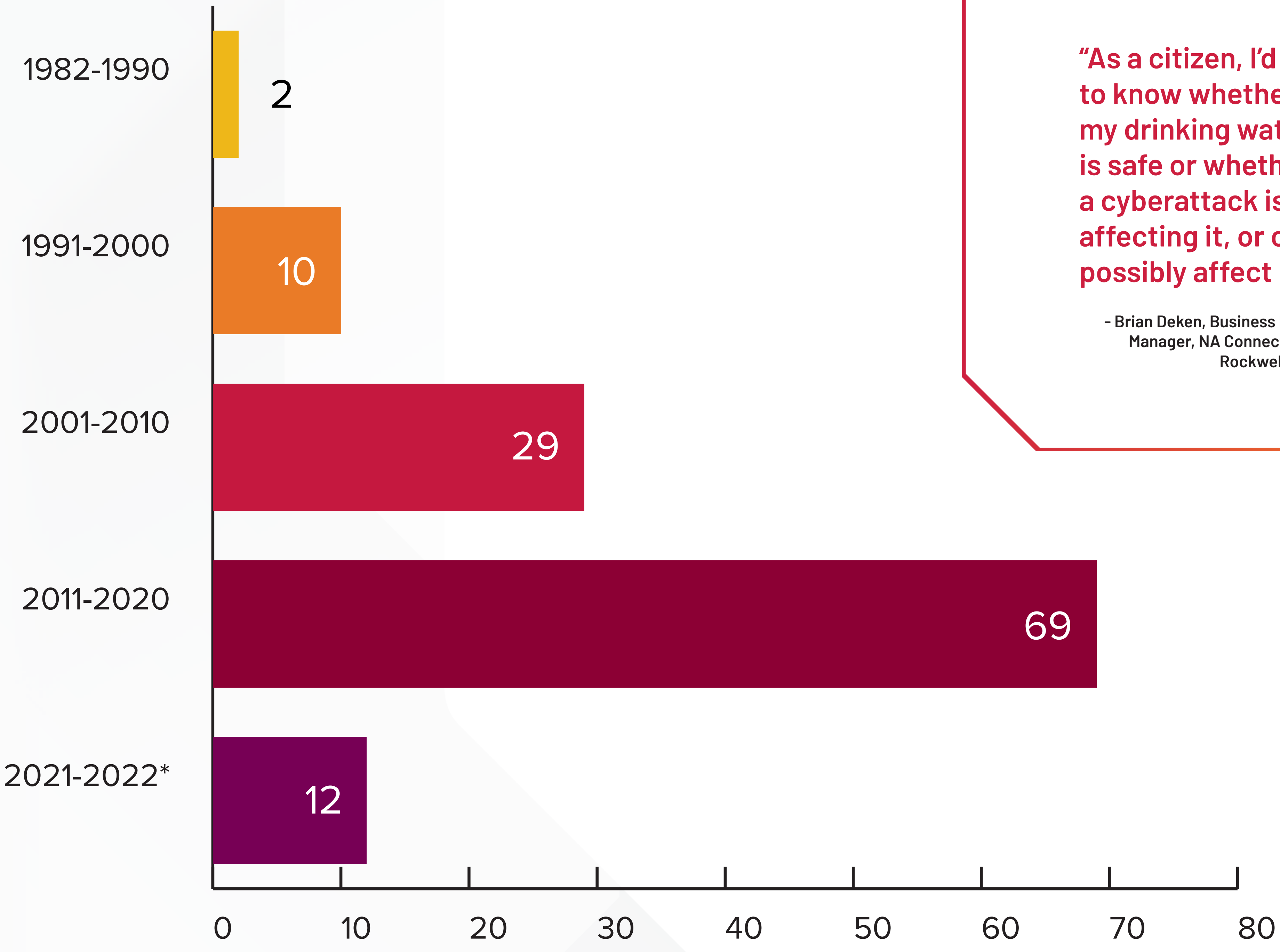
In the U.S. and across Europe, there's a rising regulatory focus on OT cybersecurity, especially for industries in Critical Infrastructure sectors. Greater regulatory oversight means that industrial organizations should evaluate their current cybersecurity protections and any potential gaps, to help them add more proactive protections that will better secure their operations against cyberattacks.

Source[2]: Reported Data Breaches in the US Reach Near Record Highs

Figure 1

Tracking OT/ICS Security Incidents

Tracking incidents 1982 - present



> "As a citizen, I'd like to know whether my drinking water is safe or whether a cyberattack is affecting it, or could possibly affect it."
>
> - Brian Deken, Business Development Manager, NA Connected Services, Rockwell Automation

Key Findings

- 60% of the OT/ICS incidents analyzed resulted in **operational disruption**.
- 40% resulted in **unauthorized access or data exposure**.
- In more than half of OT/ICS incidents, **SCADA systems** are targeted, with **Programmable Logic Controllers (PLCs)** as the next-most-common target. PLCs are industrial computers used to control different electro-mechanical processes. CISA and NSA warned about PLC targeting in an OT cybersecurity advisory.[3]
- **Broader supply chains** are also impacted approximately 65% of the time. A Japanese auto manufacturer suspended operations on 28 production lines across 14 plants, for at least a day after a key supply chain partner, a plastic parts and electronic components manufacturer, was hit by a suspected cyberattack.[4]

Rockwell Automation recommends:

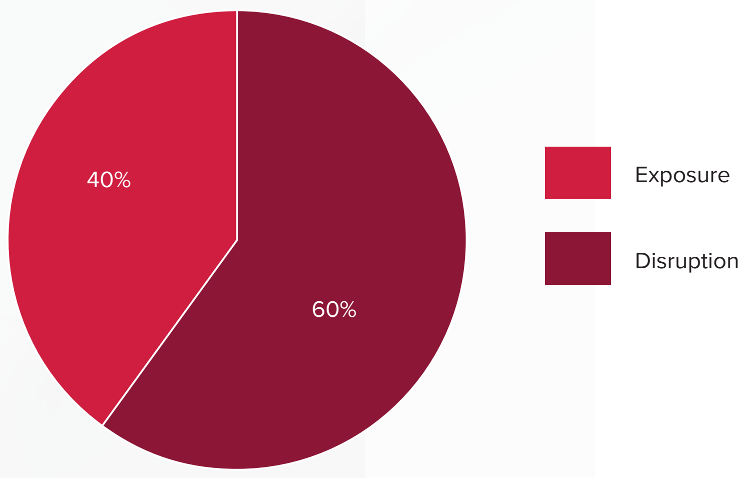
In a world where it's impossible to eliminate all cybersecurity risks, a proactive approach to critical infrastructure incident response is crucial to protect the operational continuity of essential systems and services. Rapid, well-orchestrated incident response capabilities are a must-have for bolstering resilience amidst today's most pressing threats.

Source[3]: CSA ICS Know the Opponent
Source[4]: Toyota's Supply Chain Cyber Attack Stopped Production

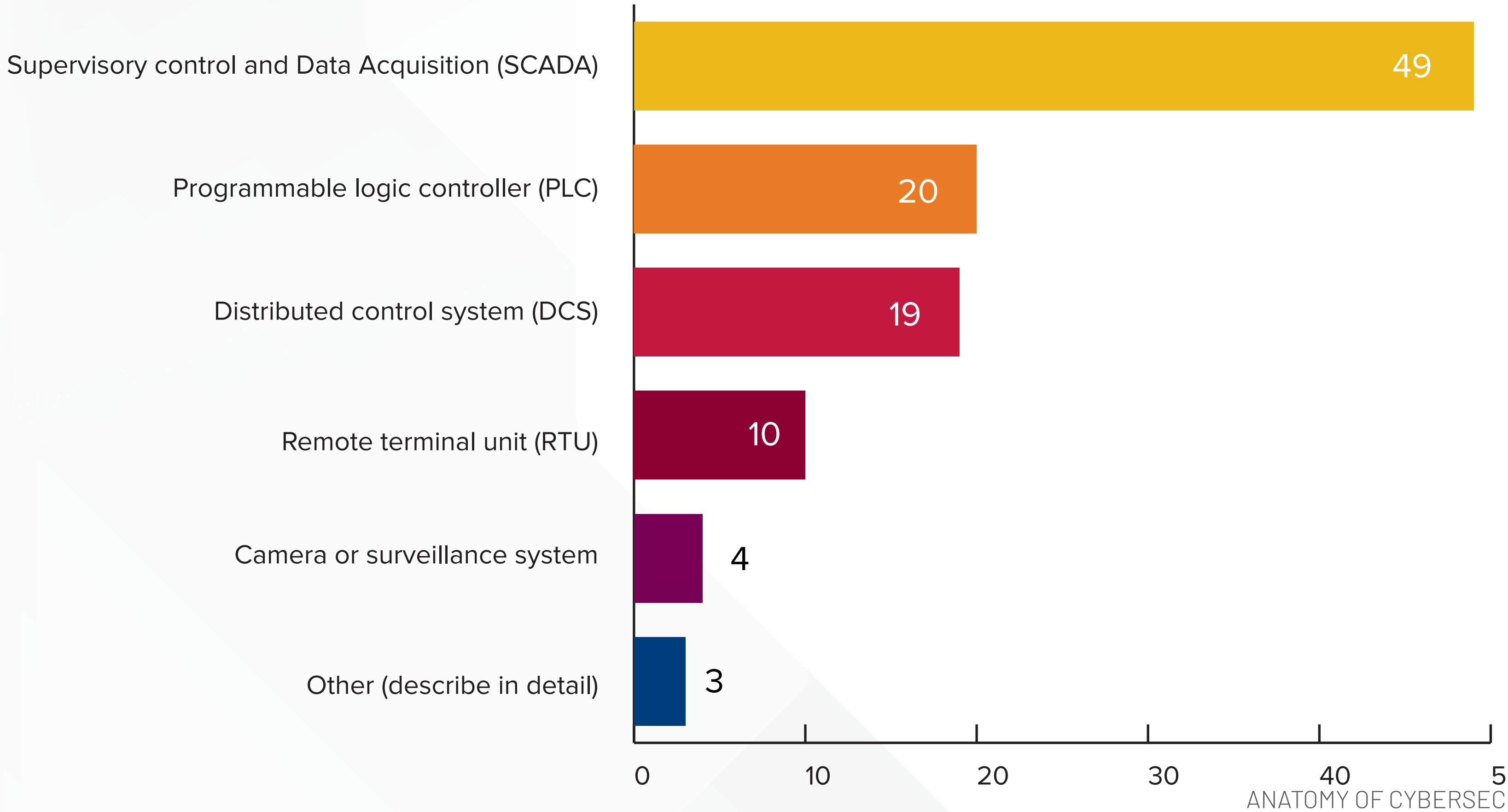
Figure 2 & 3

Understanding OT Implications

OT implications



OT/ICS technologies hit



Key Findings

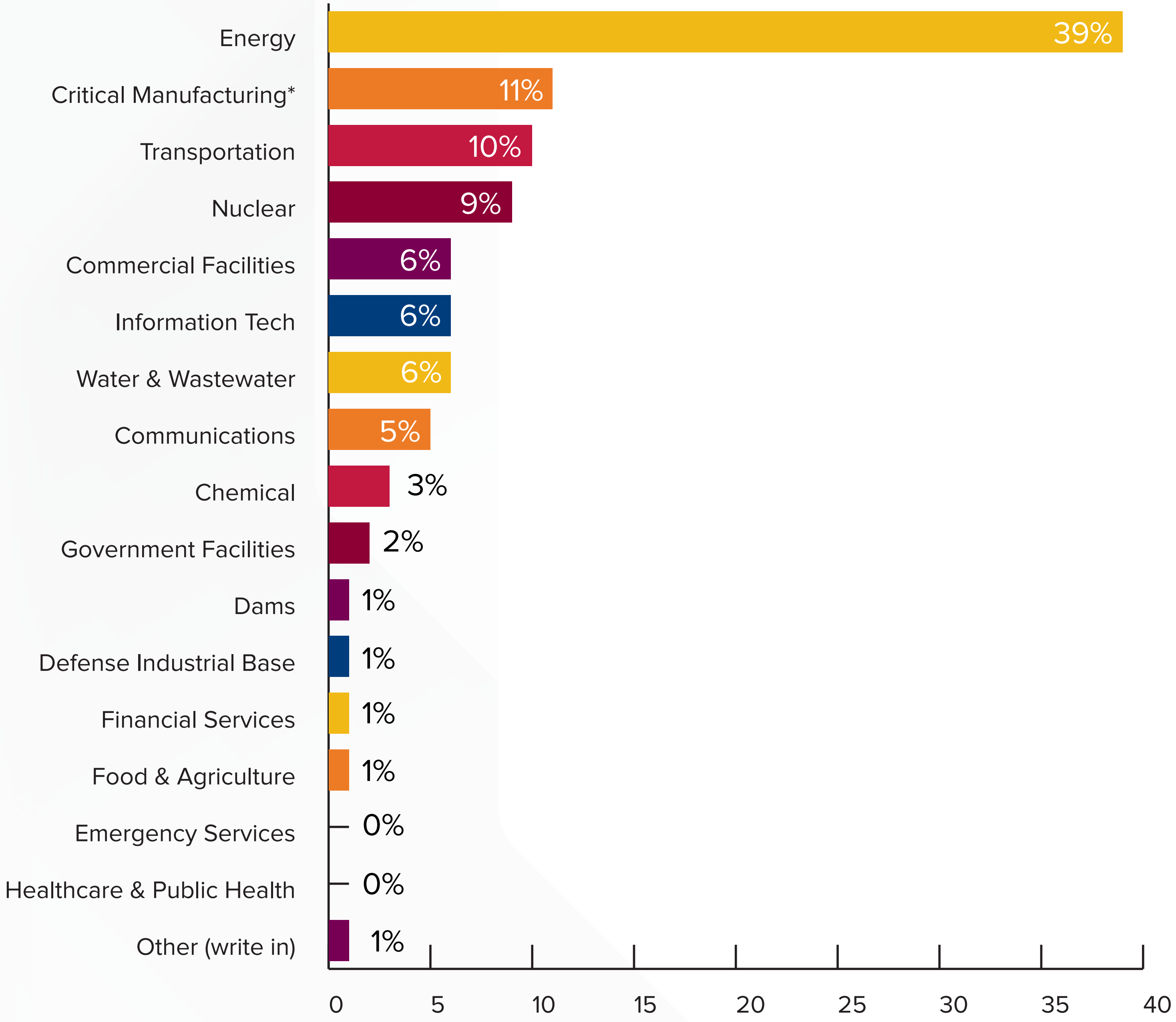
- Within this data set, the Energy sector recorded three times as many incidents as the next closest vertical. As is well reported, the potential for high impact creates greater opportunities for both ransomware payouts and for adversarial nation-state goals. However power plants, substations and related infrastructure are also aging, with many built up to 50 years ago. Older infrastructure wasn't built to leverage modern security controls.
- The U.S. government has recognized growing numbers of incidents targeting water and wastewater sectors, and has implemented emergency regulations in this and other Critical Infrastructure sectors.
- Strengthening of reporting requirements by regulatory agencies is a global trend. Governments are compelling public and private entities to disclose incidents, data theft, and ransom payments. One such regulation in the European Union is the Directive on Security Network and Information Systems.
- The 'Other' category represents the International Space Station.

A reminder: The data set analyzed includes OT/ICS incidents with enough publicly reported information for evaluation. Rockwell Automation and Cyentia remind readers to use it directionally, as conclusions are specific to the data set analyzed. Each sector differs in the number of organizations analyzed, regulatory requirements, business models, technology portfolios, and even the size of organization involved in each OT breach incident.

Figure 4

Critical Infrastructure Sectors Impacted

OT/ICS industry sectors attacked



* The Cybersecurity and Infrastructure Security Agency (CISA) identifies Critical Manufacturing to include metals, machinery, electrical and transportation equipment and services.

An Energy Sector Case Study

Digging Deeper Into an OT Incident

In 2020, a hacktivist organization called the Jerusalem Electronic Army made several social media posts claiming to have compromised control systems belonging to the public water infrastructure in Israel. The group posted screenshots of internet-facing, human-machine interfaces (HMIs), which visualize plant automation processes for operators tasked with managing these processes.

The group, ultimately, did not disrupt or damage the Israeli water supply, and instead was demonstrating its capabilities in an attempt to make a political or cultural statement.

The crux of the incident, however, was the web-based HMI interface that was not password-protected. This is a gold mine for an attention-seeking hacktivist adversary, and potentially devastating in the hands of a technically advanced adversary that is much less likely to advertise its access to critical systems and processes.

Enumerating internet-facing control systems is relatively simple via a Censys or Shodan search. Even password-protected infrastructure can be brute-forced, requiring defenders to rely on two-factor authentication, hardware tokens, and other defense-in-depth measures to blunt the effects of these types of attacks.

The risk of internet-facing HMI interfaces, for example, includes affording a threat actor direct access to the physical process at Level 0 of the Purdue Model for ICS. This is inherently a risk not only to process availability but also to physical safety. Defenders must understand their exposure and mitigate risks through strong authentication and secure remote access.

The MITRE ATT&CK framework is valuable to industrial organizations seeking to improve their cybersecurity posture. The framework provides a comprehensive overview of the tactics and techniques that adversaries use to compromise systems. It's primarily used to identify and prioritize security risks. According to a 2022 survey by the SANS Institute, MITRE ATT&CK for ICS is the most widely used ICS framework, with 70% of respondents saying that they use it. It's used globally by organizations of all sizes and types, including government agencies, law enforcement, and security vendors. The MITRE ATT&CK for ICS framework is free to use, and is constantly being updated with new information about adversarial tactics and techniques.

Key Findings

- **More than 80%** of events started with an **IT system compromise**. This is attributed to increasing interconnectivity; most OT networks communicate with the outside world via an IT network. In addition, attackers increasingly leverage internet-facing systems such as human-machine interfaces (HMIs) and engineering workstation applications, which are prime targets.
- This underscores the importance of **proper network architecture** to support enterprise security in this era of rising industrial connectivity. If you don't set up networks properly, keep OT networks segmented and air-gapped, along with other best practices such as ongoing employee security awareness training - the potential for attack increases.

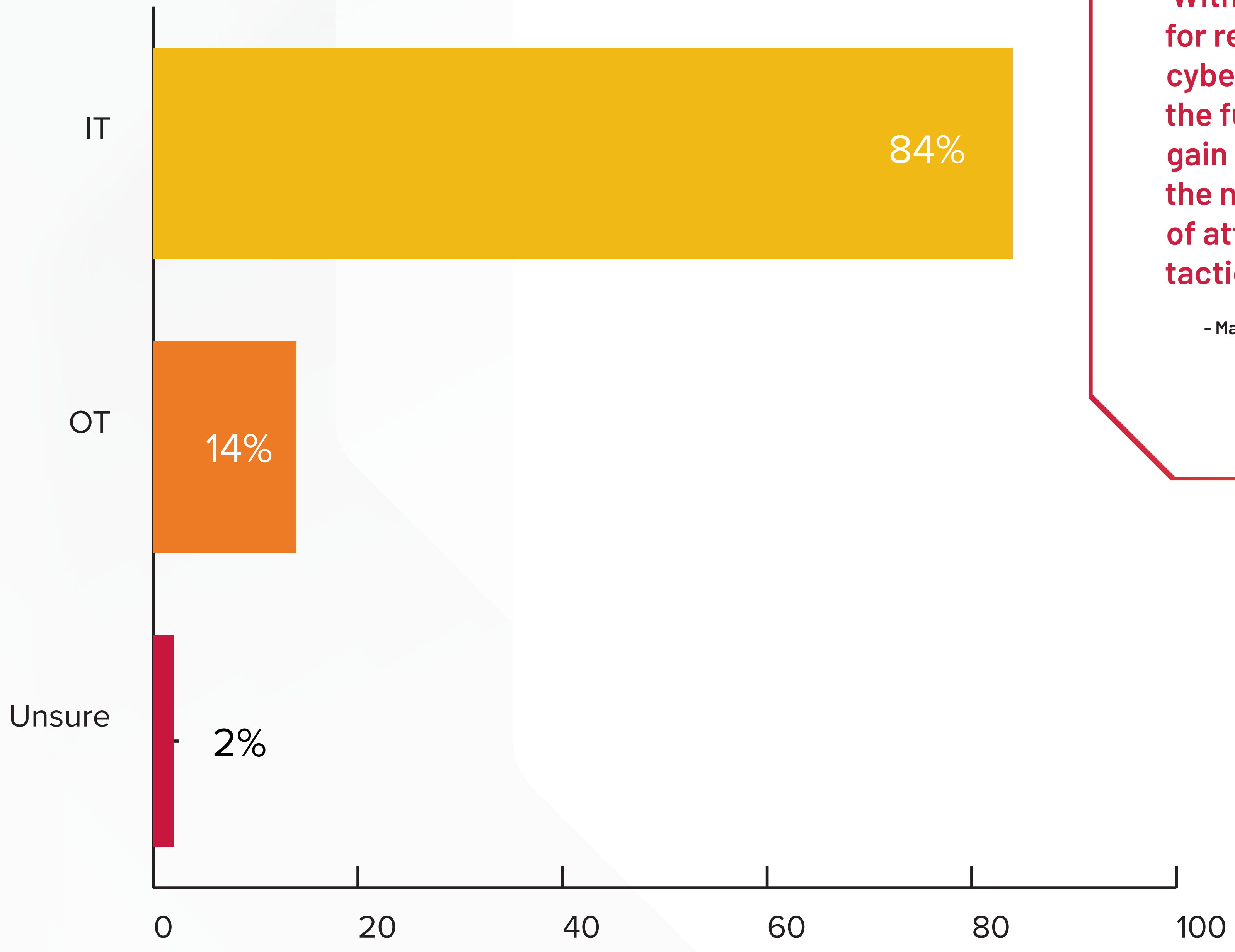
Rockwell Automation recommends:

As our understanding evolves, so too does the need for stronger OT security protections. Putting in a firewall between IT and OT environments is no longer enough to properly separate IT from OT to protect against attacks. Same goes for remote access. There are standard practices, such as passwords, that are being thwarted regularly by attackers. Without greater protection, endpoints will contribute to infiltration. Additional counter-measures must be considered, to include a well-defined Incident Response plan that can help your organization quickly respond and recover from cybersecurity incidents.

Figure 5

IT Dominates Initial Point of Entry

Initial point of entry



> "With stricter requirements for reporting OT cybersecurity incidents in the future, we can expect to gain invaluable insight into the number and severity of attacks, as well as the tactics and defenses used."
>
> - Mark Cristiano, Commercial Director, Global Cybersecurity Services, Rockwell Automation

Key Findings

- **More than 80%** of attackers come from **outside the organization**.
- **Insiders play an 'indirect' role** in more than one-third of incidents. The 'indirect' role insiders play is primarily becoming a victim of a **phishing attack.**
- **Nearly 60% of attackers in this Cyentia research study come from nation-state affiliated groups**. Many attacker identities and regional locations are hidden. Threat actors go to great lengths to conceal this information.
- The most common motives reported are **politically or financially** driven.

A Few Definitions:

Air-gapping: a network security measure employed to ensure a computer or network is secure by physically isolating it from unsecured networks.

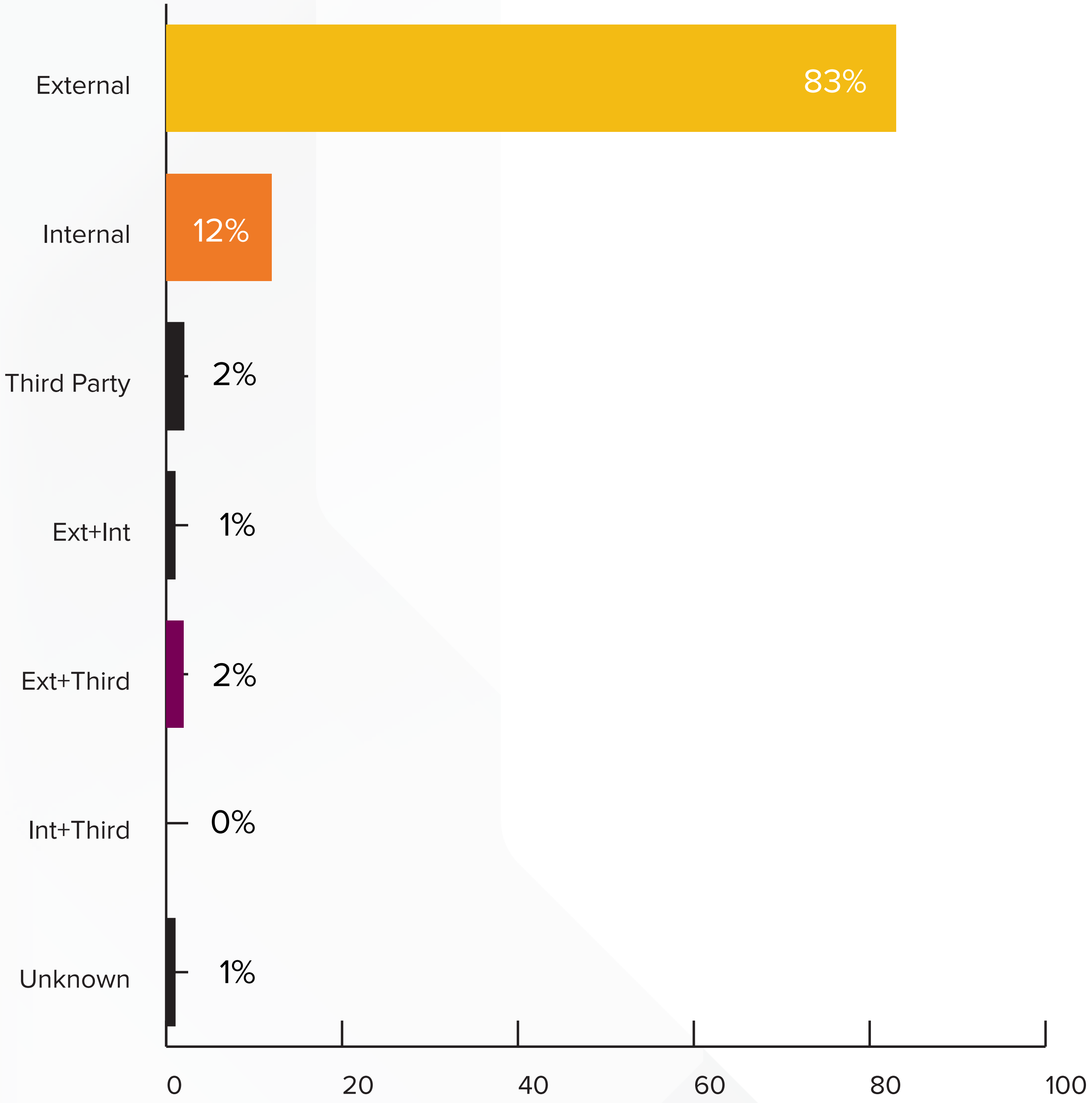
Segmentation: a layer of physical security that cordons off a network from other networks, separating an OT network from an IT network, a guest network from a corporate network, or one critical manufacturing network from another.

Zero Trust: a security framework requiring all users, whether in or outside the organization's network, to be authenticated, authorized, and continuously validated for security configuration and posture before being granted or maintaining access to applications and data.

Figure 6

Profiling Threat Actors

Actor categories



Please note, in this chart:
External = anyone outside the organization
Third party = a contractor, vendor, supplier or other partner
Internal = employees or other insiders, those considered members of an organization

Key Findings

- The percentage of **attacks attributed to nation-state affiliated groups** is higher than in other studies, at **nearly 60%** of all attacks in this sample. In other research, the Cyentia Institute has found just over 1% of cyberattack events are attributable to nation-state actors.
- However, while surprising, it's not illogical given that nation-state attackers most often want to impact critical infrastructure, supply chains, exfiltrate data from critical systems, or simply take OT systems offline.
- In one notorious 2020 attack, Russian state-sponsored actors used system vulnerabilities to hack into more than 200 systems. Attackers used credentials from at least three organizations to carry out the attack, impacting multiple U.S. government systems, NATO, the U.K., and European Union systems. The U.S. imposed sanctions on Russia as a result.[5] The impact of having international government data, infiltrated AND exfiltrated will take years to completely understand.

Countries of Origin:

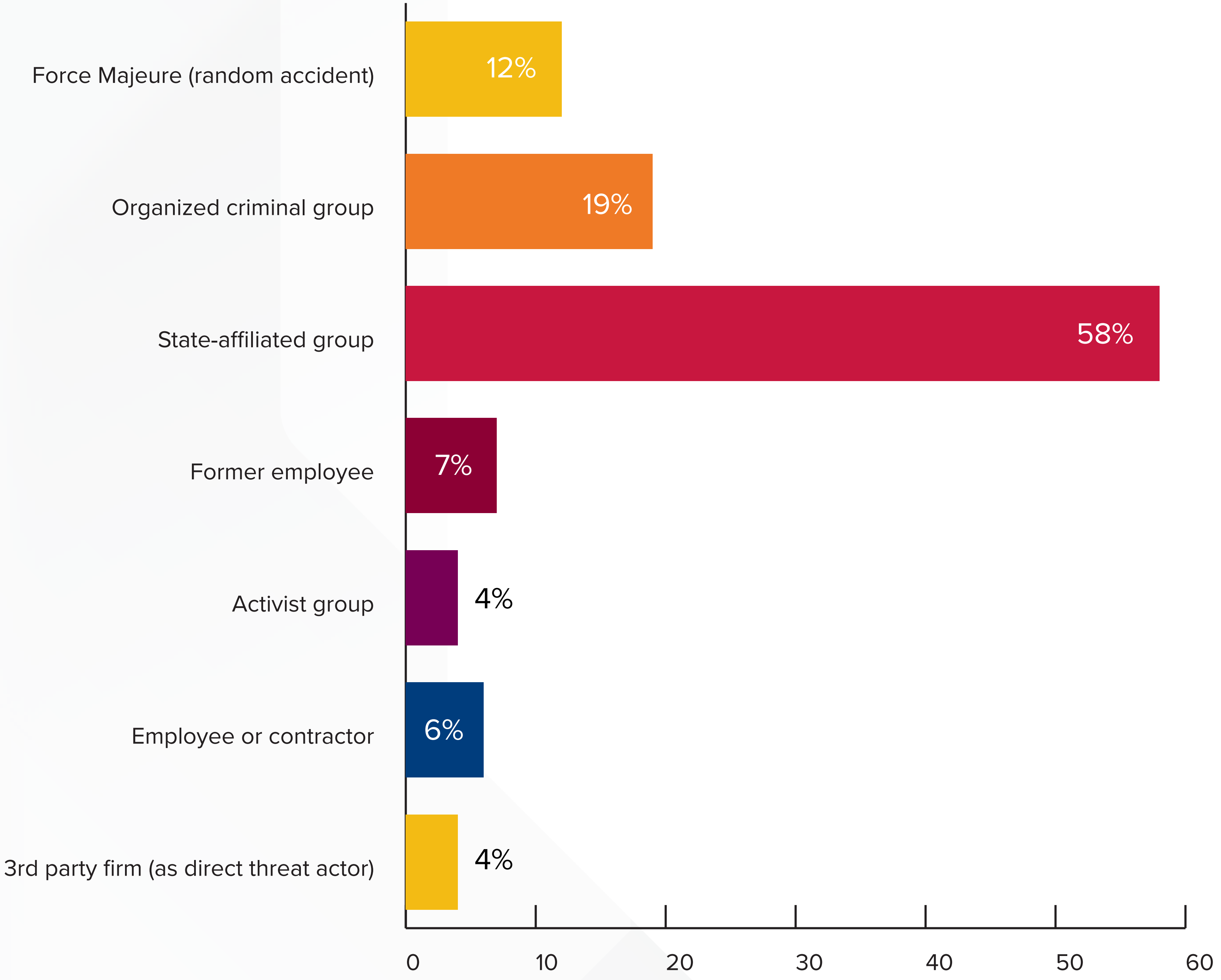
Globally, the countries of origin included in Cyentia's Advisen OT research study are the following: Australia, Belarus, Canada, China, Finland, France, Germany, Great Britain, India, Iran, Iraq, Ireland, Israel, Italy, Japan, Liberia, Lithuania, Luxembourg, Russia, Saudi Arabia, Sweden, Switzerland, Taiwan, Türkiye, Ukraine, the United States.

Source[5]: SolarWinds Attackers Accessed US Attorneys Office Emails

Figure 7

Digging Deeper into Attack Personas

Threat actor types



Key Findings

- **Phishing reigns** as the easiest, most successful initial access (attack) technique. Phishing has grown to include email, online, SMS/text messaging and voice/telephony, making it a powerful weapon for cybercriminals.
- **External remote services** ranked second as an initial access method for both IT and OT events. While the intent is to give legitimate users remote access, this has become a gateway for attackers, especially since 2020.
- **Smart targets:** As sophistication rises, anything 'smart' on your network becomes a target. The use of up to real-time network asset inventories, 24/7 threat detection, and appropriate policies and procedures around removable media – among other best practices - can help prevent an IT attack from migrating to OT, with the potential to shut down an organization's supply chain, processes, or even an entire physical plant.

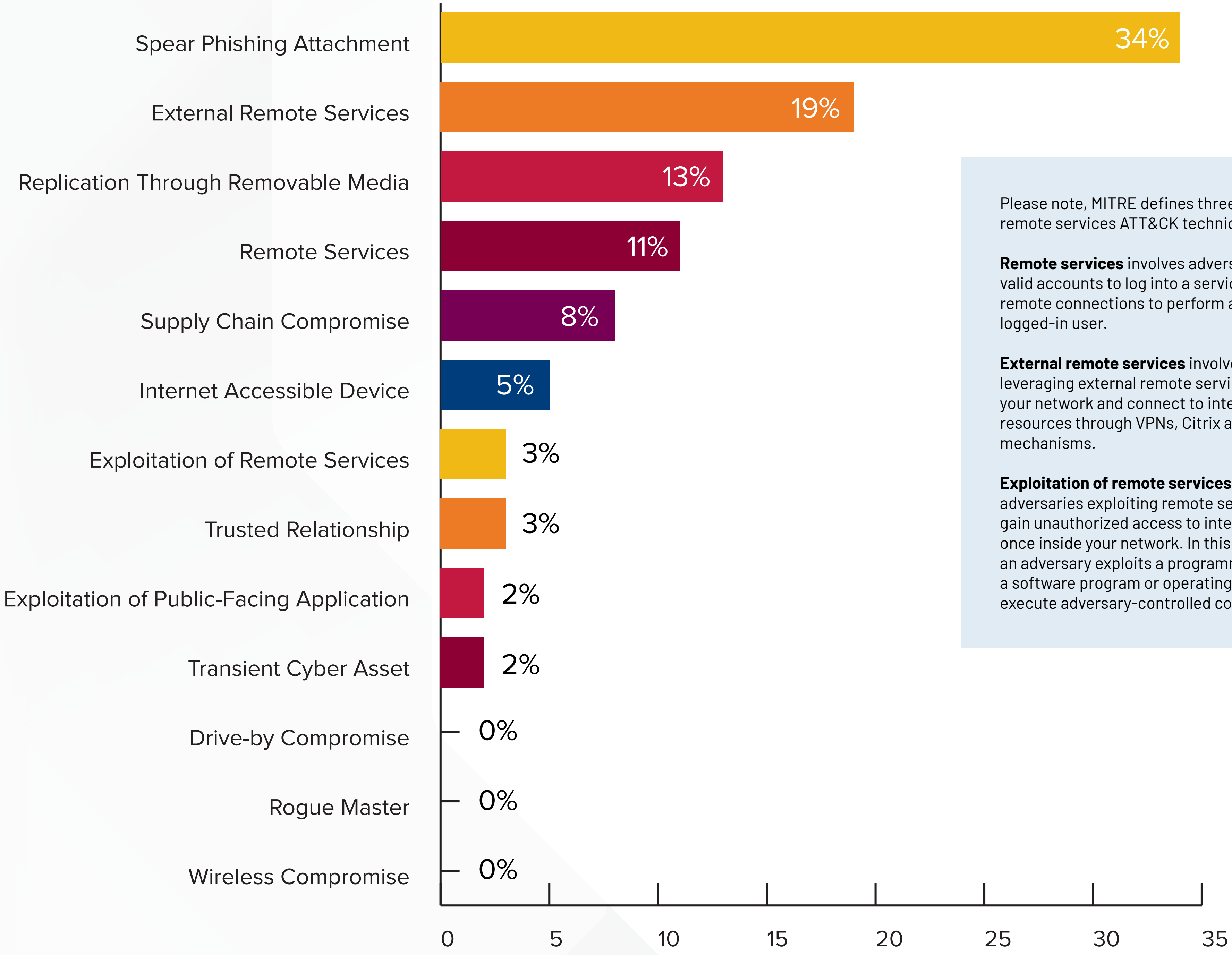
Rockwell Automation recommends:

To defend against OT attacks, use a variety of tactics such as segmentation, air gapping and Zero Trust. If you can imagine someone already inside your organization moving laterally against you, what countermeasures would you take? One quick tactic is to change passwords, as default credentials offer an easy opening for attackers. It's important to think about defense-in-depth, using multiple practices and solutions to protect yourself and your OT environment.

Figure 8

Spear Phishing Tops Access Techniques

Initial access techniques for OT incidents



Please note, MITRE defines three seperate remote services ATT&CK techniques:

Remote services involves adversaries using valid accounts to log into a service that accepts remote connections to perform actions as a logged-in user.

External remote services involves adversaries leveraging external remote services to access your network and connect to internal network resources through VPNs, Citrix and other access mechanisms.

Exploitation of remote services involves adversaries exploiting remote services to gain unauthorized access to internal systems once inside your network. In this scenario, an adversary exploits a programming error in a software program or operating system to execute adversary-controlled code.

Key Findings

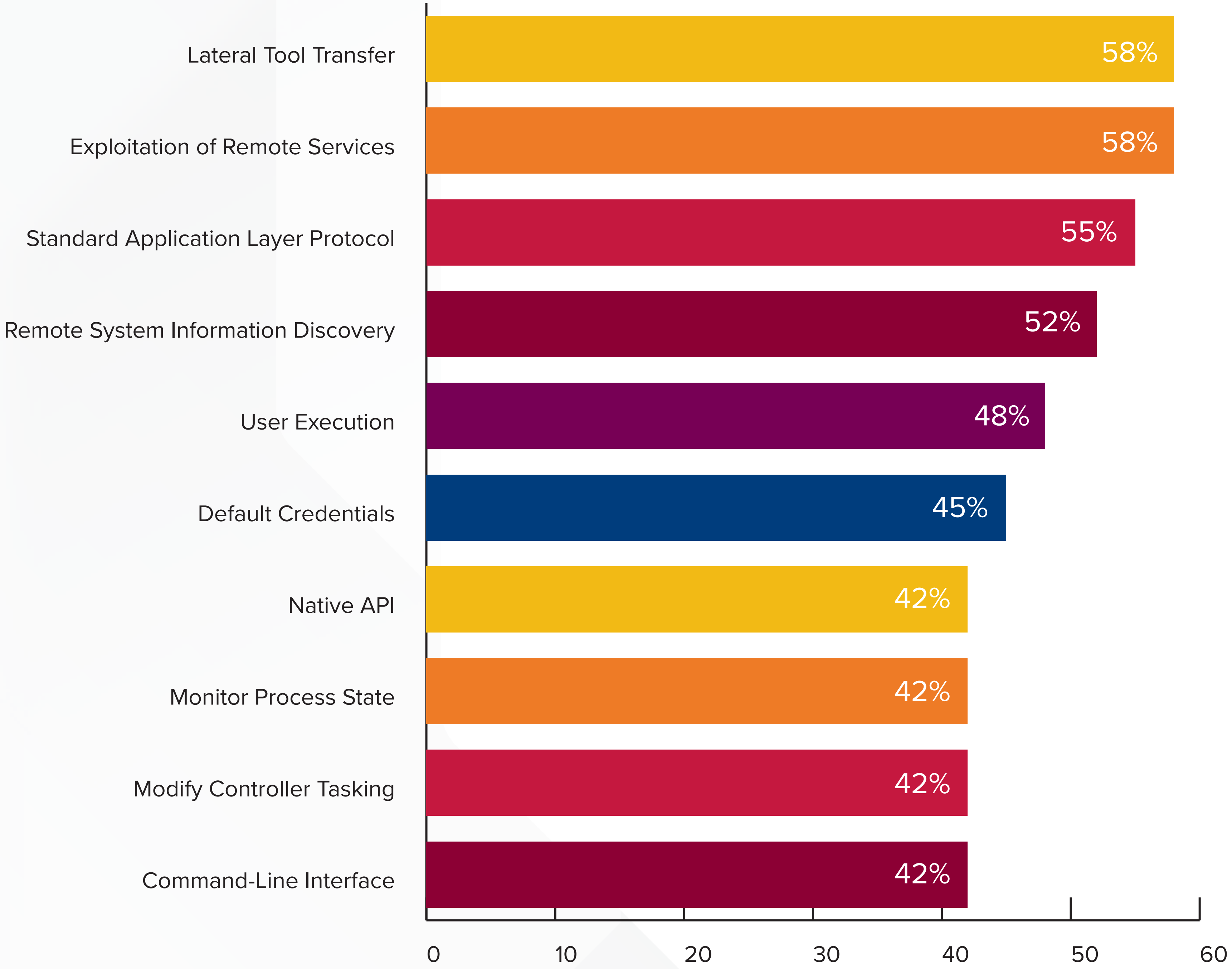
- According to MITRE, "ATT&CK for ICS focuses on adversaries who have a primary goal of disrupting an industrial control process, destroying property or causing temporary or permanent harm or death to humans by attacking industrial control systems."
- In IT environments, attacks typically begin with **network discovery**, which is used to help attackers learn and understand where assets are located and how to get to them.
- In OT, attackers most often attempt to **directly impact industrial processes**. Many seek to disrupt operations for monetary gains, such as ransom payments, or for other outcomes involving economic or militaristic advantages. The number of U.S.-based threat actors attacking industrial organizations grew by 35% in 2022, driving an 87% increase in breaches over the same period.[6]
- Attackers use **Lateral Tool Transfers, Exploitation of Remote Services and Standard Application Layer Protocols** to manipulate an operator's view, and in many cases, take control over specific OT processes.

Source[6]: ICS Cybersecurity Year in Review Executive Summary 2022

Figure 9

Once Inside, OT Attackers Aim to Control & Disrupt

Post-compromise MITRE ATT&CK techniques



Key Findings

Data exfiltration tops enterprise impacts

When attacks happen that disrupt business, the impacts are widely felt. It doesn't take a WannaCry-style incident for organizations to be negatively impacted.

Let's take a look at the impact of these ATT&CK designations - starting in the MITRE enterprise framework for comparison. In 'Exfiltration over C2 Channel' attacks, adversaries steal data and then exfiltrate it using an existing command and control channel, which is the primary way that such incidents impact enterprise operations.

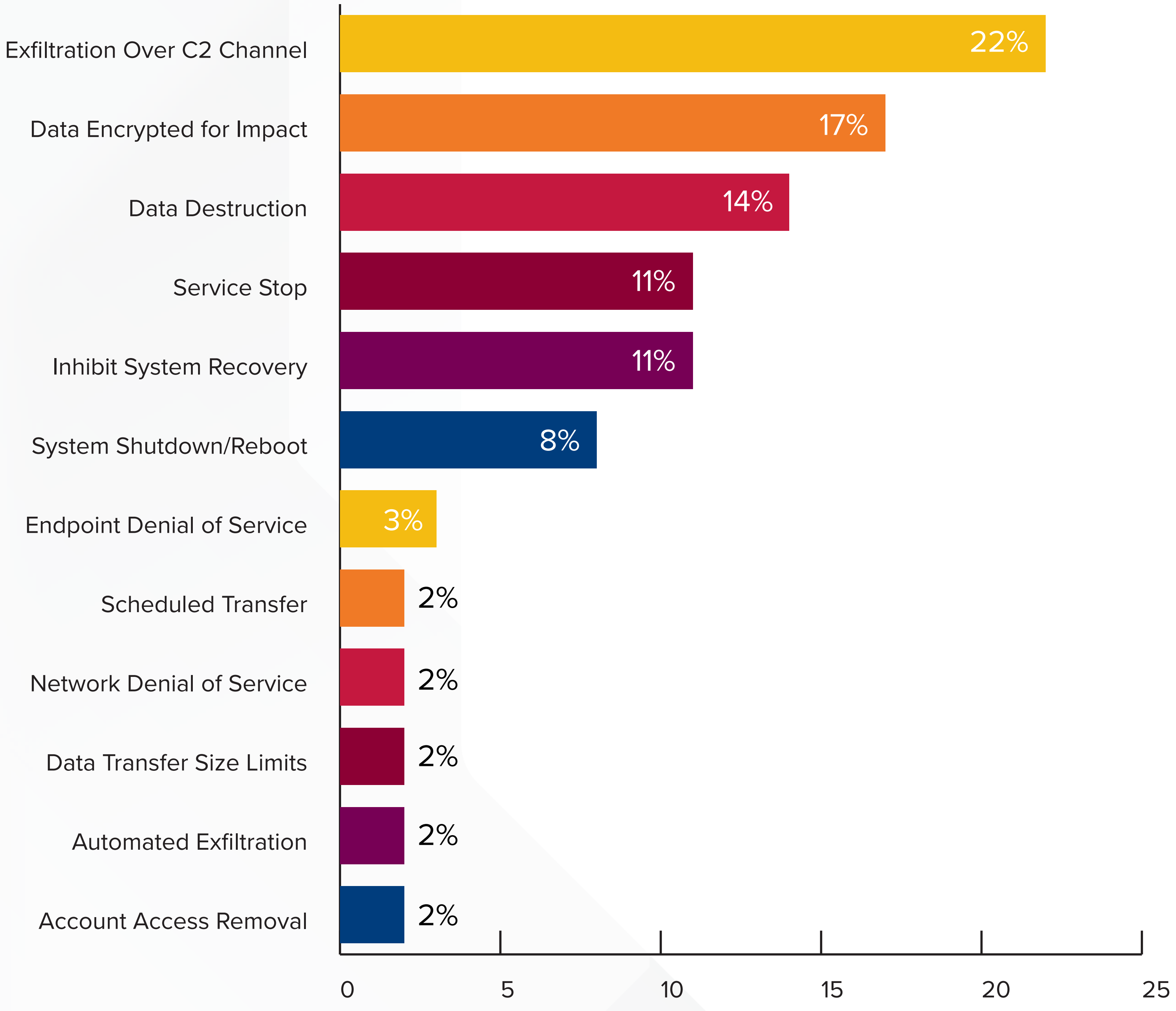
Two other attack types, 'Data Encrypted for Impact' and 'Data Destruction Techniques,' round out the top three ways that cyberattacks impact enterprises. Taken together, the top three MITRE ATT&CK techniques shown in the chart are most commonly associated with ransomware attacks.

This becomes clearer when looking at the impact on ICS designations.

Figure 10

Additional Attack Implications

Post-compromise MITRE ATT&CK techniques



Key Findings

ICS impacts: control, then disrupt

'Manipulation of View' and 'Manipulation of Control' are the top two methods used to impact ICS environments. The numbers here are directly tied to the incidents analyzed in this study.

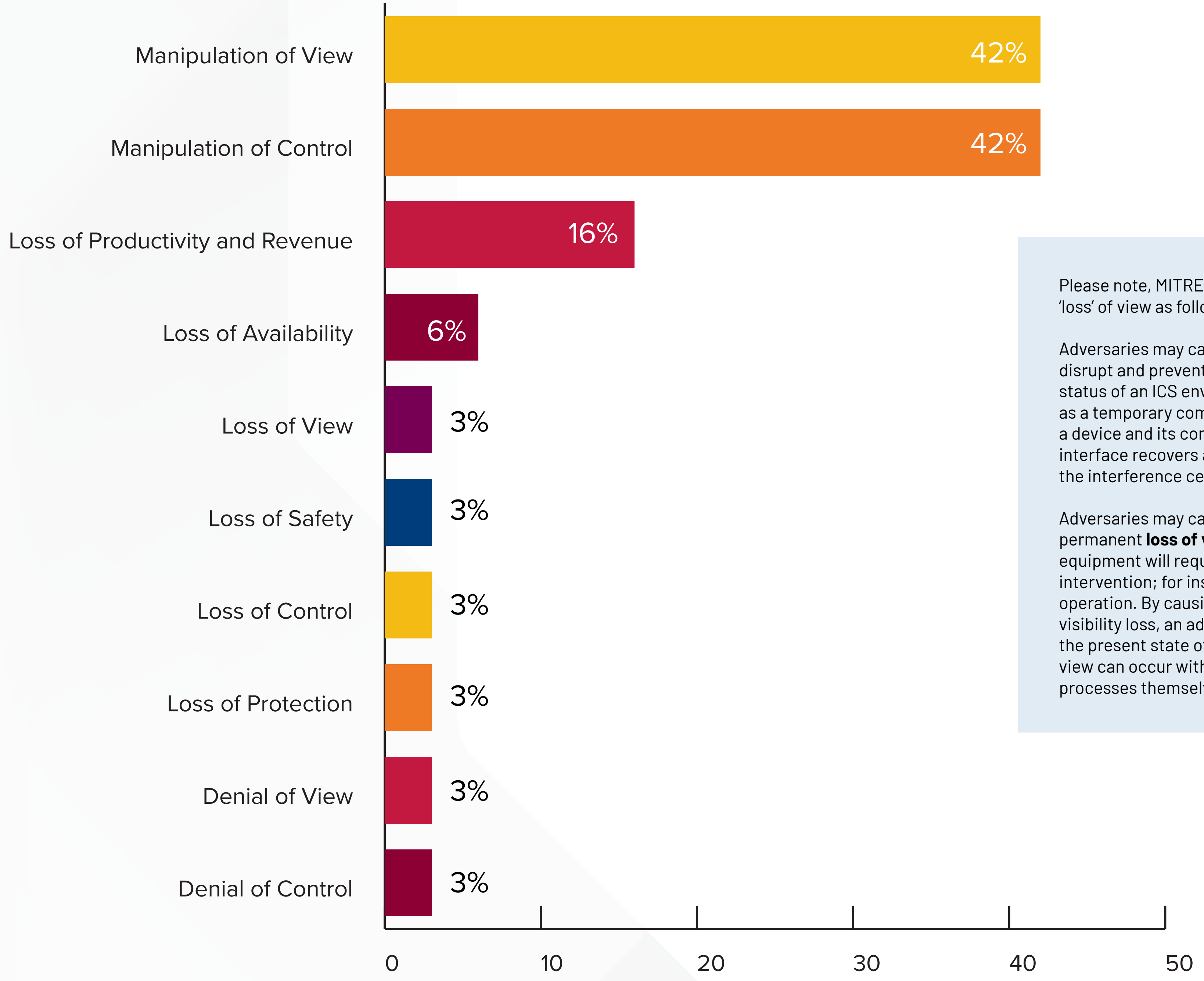
Rounding out the top three ICS ATT&CK designations is 'Loss of Productivity and Revenue.' When we connect this method to the previously mentioned Manipulation of View and Manipulation of Control attack types, it's clear to see how supply chains can be impacted in these incidents. If a malicious user manipulates the view and control of an OT/ICS system in charge of production, they may also infiltrate and impact the entire product supply chain of the organization's partners, suppliers and customers.

When we look back to the techniques used specifically in the non-energy sector, supply chain impact is one of the top three most prevalent outcomes. This far-reaching impact, well beyond an organization's borders, makes it extremely important for organizations across all industries to protect against cyberattacks.

Figure 11

Additional Attack Implications *continued*

Post-compromise MITRE ATT&CK techniques



Please note, MITRE defines 'denial' and 'loss' of view as follows:

Adversaries may cause a **denial of view** to disrupt and prevent operator oversight on the status of an ICS environment. This may manifest as a temporary communication failure between a device and its control source, where the interface recovers and becomes available once the interference ceases.

Adversaries may cause a sustained or permanent **loss of view** where the ICS equipment will require local, hands-on operator intervention; for instance, a restart or manual operation. By causing a sustained reporting or visibility loss, an adversary can effectively hide the present state of operations. This loss of view can occur without affecting the physical processes themselves.

Reflections & Recommendations

This report has examined a selection of Advisen's Cybersecurity Loss Database to better understand patterns around historical OT/ICS cybersecurity incidents. Our goal has been to gain a better understanding of where we've been, and more importantly, to better forecast where attacks in this category are headed and the level of defenses that will be needed in the years ahead.

With more systems, networks and devices being connected in OT/ICS environments, as well as the legacy equipment housed in most industrial environments, many organizations are exposing new vulnerabilities to sophisticated adversaries. Having a strong, modern OT/ICS security program in place must be a part of every industrial organization's responsibility to maintain safe, secure operations and ongoing availability.

Industrial organizations must prioritize safety and reliability to protect against cyberattacks - and do so quickly. With risks and reporting mandates growing, a paradigm shift must occur. For example, many industrial organizations are often reluctant to update firmware when there are announcements of a critical vulnerability. They may even be told not to patch, as updates take systems offline and have the potential to disrupt supply chains. Yet the risk to OT infrastructure can be so much worse.

Today, relatively efficient solutions are possible for OT/ICS cybersecurity. Minutes matter and seconds count, so start today. Rockwell Automation and our network of world-class partners are ready to advise you.

Tips and advice

To get started strengthening OT cybersecurity:

- Focus on **defense-in-depth**, including pulling from structures such as **Zero Trust** and the **NIST Cybersecurity Framework**.
- Secure **remote access**, through stronger passwords and **multifactor authentication.**
- **Monitor** for threats 24/7.
- **Segment IT and OT** to make the most of firewall configurations that will help you keep IT attacks from bleeding into OT environments.
- **Continuously train** your internal staff to keep up with the latest phishing scams and how to avoid them.

Looking Ahead: Rising Regulatory Requirements

Governments around the globe are compelling public and private sector entities to disclose cybersecurity incidents, data theft, and ransom payments to reverse chronic underreporting of cybercrimes, and to help mitigate risks.

U.S. companies operating in Critical Infrastructure sectors must now report breaches, under the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA), instead of being encouraged to do so voluntarily.

This strengthening of reporting requirements is a global trend. In the E.U., the Directive on Security Network and Information Systems – along with a host of other regulations – mandate that Critical Infrastructure providers report breaches. On a global scale, the United Nations is discussing the parameters of an international treaty focused on individual data protection as well as cyber resilience.

As threats increase, we expect to see increasing pressure on regulators to issue more rules about disclosure and cyber risk mitigation.

Sources:
CIRCIA https://www.cisa.gov/circia
E.U. regulation, https://digital-strategy.ec.europa.eu/en/policies/nis2-directive
Additional regulations: https://www.enisa.europa.eu/topics/incident-reporting
U.N., https://unric.org/en/a-un-treaty-on-cybercrime-en-route/

Acknowledgements

About Cyentia

The Cyentia Institute is a research & data science firm with a mission to advance knowledge in the cybersecurity industry. We accomplish this by partnering with vendors and other organizations to publish a range of high-quality, data-driven research. Cyentia's exclusive partnership with cybersecurity publisher and education firm ISMG provides robust data-based and survey research and analysis to help the cybersecurity community lower risks and stay on top of the latest threats.

About Rockwell Automation

Rockwell Automation provides a range of industrial security solutions and services to help you manage threats and boost the resiliency of your OT and IT ecosystem. Our experts can help you build a robust and secure network infrastructure while helping to defend against threats and rapidly respond to incidents.

In addition to deep expertise and knowledge of the latest best practices, we bring production operations wisdom from more than 120 years in industrial automation. Our worldwide locations enable customers to apply cybersecurity protections on a global scale across multiple sites with logistics as finely tuned as you'd expect from the industry leader in industrial automation.

Get in touch with us to learn more.

REACH OUT TO TALK TO AN EXPERT TODAY

WATCH OUR WEBINAR TO LEARN MORE ABOUT THIS RESEARCH STUDY

In partnership with Cyentia Institute

Rockwell Automation

Connect with us.

rockwellautomation.com

expanding **human possibility**®

AMERICAS: Rockwell Automation, 1201 South Second Street, Milwaukee, WI 53204-2496 USA, Tel: (1) 414.382.2000, Fax: (1) 414.382.4444
EUROPE/MIDDLE EAST/AFRICA: Rockwell Automation NV, Pegasus Park, De Kleetlaan 12a, 1831 Diegem, Belgium, Tel: (32) 2 663 0600, Fax: (32) 2 663 0640
ASIA PACIFIC: Rockwell Automation, Level 14, Core F, Cyberport 3, 100 Cyberport Road, Hong Kong, Tel: (852) 2887 4788, Fax: (852) 2508 1846

Publication GMSN-SP025A-EN-P-August 2023