Whitepaper

Plan to Recover from an Industrial Cyber Attack

WHAT TO HAVE IN PLACE WHEN THE WORST HAPPENS

With increasingly interconnected systems and exponentially growing quantities of data, industrial operations must consider not if *a cyber attack will occur, but how to respond* when *it does. Robust data and software system management can prevent production downtime during normal operations and ensure resilient recovery when the worst occurs.*

By Jack Smith, Automation.com

AUTOMATION.COM | ISA A subsidiary of the International Society of Automation

AUVESY-MDT

Cyber risks are on the rise. Manufacturing and industrial operations long ago shed their belief that they were invulnerable because their systems were too isolated or too obscure to be targeted. Organizations now seek to understand the impact and likelihood of their cybersecurity risks and then seek to reduce those risks. But mitigating risk is only the first part of comprehensive cybersecurity planning.

To enable continuous operations and limit business impact when a cyber attack does occur, organizations need additional tactics. These can include strategically hiring cybersecurity talent or using new methods to identify, combat, and recover from attacks. Given increasingly interconnected and frequently updated systems, robust software system management is a particularly useful tool.

Rise of OT cyber risks

Improvements to a plant's operational technology (OT) cyber risk management and mitigation plans should be made in tandem with the rise of attacks, which are up 144% from 2020, according to Industrial Safety & Security Source (ISSSource). Data from the company's OT Security Incidents in 2021: Trends & Analyses report, which analyzes data from its ICSSTRIVE.com database, says "the year 2021 saw the number of cyber attacks with physical consequences in process and discrete manufacturing industries more than double over those reported in 2020.... Almost all these incidents were the result of targeted ransomware. Almost all these attacks impacted multiple physical sites."

In a recent webinar, ISSSource reported that OT ransomware incidents with physical consequences have increased 133% year-over-year since 2020, and that published estimates cite up to $140 million in damage per event. The types of facilities subject to these attacks cover the industry spectrums (Figure 1).

McKinsey & Co. expects that, over the next three to five years, three major cybersecurity trends will have the biggest implications for organizations of all types:

1. **Growing on-demand access to ubiquitous data and information platforms.** Organizations are collecting vast amounts of customer and machine data and are increasingly using the cloud for storing, managing, and protecting these data.
2. **A growing regulatory landscape and continued gaps in resources, knowledge, and talent.** "Many organizations lack sufficient cybersecurity talent, knowledge, and expertise—and the shortfall is growing. Broadly, cyber risk management has not kept pace with the proliferation of digital and analytics transformations, and many companies are not sure how to identify and manage digital risks," McKinsey says.

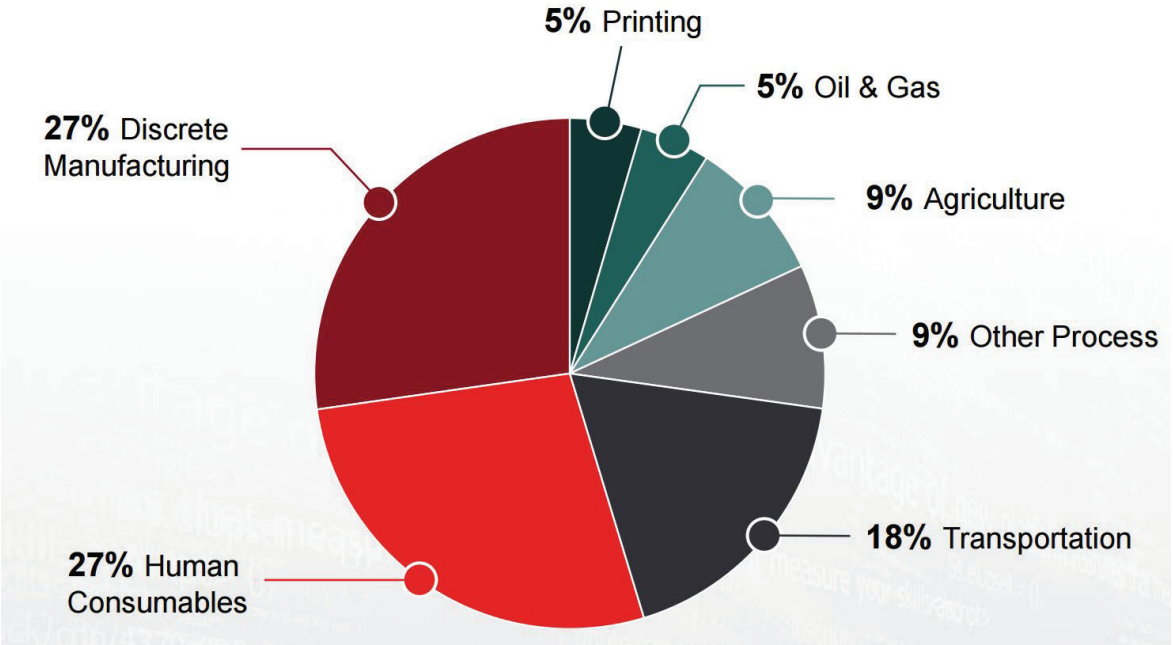

Figure 1. Cyber attack distribution by industry. *Courtesy: Industrial Safety & Security Source*

3. **Hackers are using AI, ML, and other technologies to launch increasingly sophisticated attacks.** "The stereotypical hacker working alone is no longer the main threat. Today, cyber hacking is a multibillion-dollar enterprise, complete with institutional hierarchies and R&D budgets. Attackers use advanced tools, such as artificial intelligence, machine learning, and automation," McKinsey says. "Other technologies and capabilities are making already known forms of attacks, such as ransomware and phishing, more prevalent."

Preparing for the inevitable

Automation can be used to counter more of the sophisticated attacks coming at organizations, says McKinsey. "Automation should focus on defensive capabilities like security operations center (SOC) countermeasures and labor-intensive activities, such as identity and access management (IAM) and reporting. AI and machine learning should be used to stay abreast of changing attack patterns. Finally, the development of both automated technical and automatic organizational responses to ransomware threats helps mitigate risk in the event of an attack."

As the level of digitization accelerates, organizations can use automation to handle lower-risk and rote processes, freeing up resources for higher-value activities, McKinsey advises. Automation decisions should be based on risk assessments and segmentation to ensure that additional vulnerabilities are not created. For example, organizations can apply automated patching, configuration, and software upgrades to low-risk assets but use more direct oversight for higher-risk ones.

Organizations can apply automated patching, configuration, and software upgrades to low-risk assets but use more direct oversight for higher-risk ones.

As ransomware attacks increase, organizations must respond with technical and operational changes, adds McKinsey. "The technical changes include using resilient data repositories and infrastructure, automated responses to malicious encryption, and advanced multifactor authentication to limit the potential impact of an attack, as well as continually addressing cyber hygiene. The organizational changes include conducting tabletop exercises, developing detailed and multidimensional playbooks, and preparing for all options and contingencies—including executive response decisions—to make the business response automatic," the report states.

Software system change management

Regardless of their sector, size, or task set, industrial production environments require complex information technology (IT) setups designed to handle integrated systems and high volumes of data. While both OT and IT departments use digitalization to improve productivity and other business outcomes, sometimes the two worlds require translation and teamwork so their different methods and best practices can be achieved. For example, although it has become standard practice for IT departments to schedule routine backups and manage data storage, OT personnel have been slow to adopt such data hygiene and software system management solutions.

Ensuring that the correct, authorized versions of software are always running is paramount to keeping production running—whether OT or IT personnel are tasked with managing the system.

With version control and change management tools, operators access the most current software and know when changes require further action. Advanced software solutions can summarize the entirety of an automated production environment and analyze devices on the shop floor. Because they can detect differences in programming configuration and firmware versions, even for identical sensors, such systems make it easier to isolate errors.

Change management is a structured process for planning and implementing new ways of operating. According to an article in the April 2022 issue of InTech, the official publication of ISA—International Society of Automation, "An automated, standards-based documentation process saves time and cost while increasing quality. With standards-driven processes and workflows comes the assurance of following the best industry practices during the definition, design, development, integration, documentation, and support of automation projects. This ensures the execution of projects with precision and standardization."

Successful change management relies on four core principles:

- Understanding change or changes to be made.
- Planning the best way for the necessary changes to occur.
- Implementing changes in the most effective manner.

- Communicating the implemented changes to the appropriate stakeholders.

That's just the beginning. If changes are made by multiple people to OT-centric code, the potential exists for one group to not know what another group is doing. If changes that affect the operation—and/or cybersecurity—of a manufacturing facility are made, they must be made for a valid reason. There must be documented justification for the change. If a robust change-management system is in place, that system should track and catch any deviation from what is expected in the procedures or code. The system's activity history will reveal who changed what, where, when, and why.

Good change management is not a one-and-done proposition, nor is it best executed by spot checking. **Good change management must be in place continually—in real time.** Whether unauthorized changes come from lack of employee communication, unauthorized OT system users, or actual cyber malfeasance, change management that's done correctly is a company's best insurance against downtime and resource for recovery.

Whether unauthorized changes come from lack of employee communication, unauthorized OT system users, or actual cyber malfeasance, change management that's done correctly is a company's best insurance against downtime and resource for recovery.

From detection to backup to recovery

Version control and software change management tools can help organizations at all stages of cybersecurity activity—from detection of vulnerabilities to recovery from attack. They can be used to ensure data is current and corresponds to the latest iteration. They can reveal data anomalies and, hence, vulnerabilities and exposures.

A state-of-the-art change management system can manage software programs and configuration settings data in a standardized way, so change history can reveal who changed what, where, when, and why. Such tools can aid the user in managing insecure protocols, misconfigurations, and other vulnerable security points, as well as provide automatic assessment of vulnerabilities, affected assets, and the entire industrial control system. Through threat detection functionality, the tool can automatically discover, protect, and manage an industrial control system's critical assets and provide users with risk and vulnerability reporting.

When a production system malfunctions for whatever reason, maintenance staff can take an average of three or four hours to track down changes using a manual approach to managing software versions. Automatic backups reduce the downtime and facilitate rapid recovery. The backups enable users to restore the last authorized version or an earlier one if that was the one running before the malfunction occurred.

When version control and software change management systems are installed on premises, on the OT network side of the factory floor, tasks from detection to backup to recovery can be automated. The system should allow for the IP addresses of assets and devices to be scanned and added to the system even if they are located below the programmable logic controller (PLC) level. The information gathered should include the device brand, manufacturer, firmware version, and where the device is physically located in the rack.

When users run an automated backup, it should also be possible to send this information to a threat analysis component, which can check the web to see if there are vulnerabilities in software components or firmware versions. It is also helpful if the threat analysis can identify unusual traffic patterns, malware, or external, unapproved access to the network.

Multi-faceted change management

An example of a state-of-the-art change management system is octoplant from AUVESY-MDT. octoplant is a data management platform that provides a vendor-independent and comprehensive view of all automation backup processes involving OT and IT. This change-management platform consists of eight solution sets tailored to specific industrial needs including threat protection, safeguarding assets, IoT device management, instant recovery, operational efficiency, business intelligence, compliance management, and education and training. According to Stefan Jesse, Group COO at AUVESY-MDT, while comparable software may only cover individual machines or partial aspects of a plant such as PLC, SCADA, and HMI, or the programming of robotics, octoplant provides visibility into the function and safety status of all plant elements.

Such comprehensive change-management platforms often have dashboards that can display the various statuses of the plant (Figure 2). Production managers can see where programs and configurations are

Figure 2. Change management software can show production managers the status of all machine programming as well as schedule automated backups. *Courtesy: AUVESY-MDT*

stored and how up to date they are, as well as the current and correct status of all machine programming, the version history of all changes, and tabular and graphical reports detailing program differences.

Automated backups can be scheduled to ensure the correct authorized version of each piece of software is always running. These backups can be applied to a single device or the entire plant, even if the facility consists of several hundred or even several thousand devices, sensors, pieces of hardware or software components, says Jesse.

Final thoughts

Cyber attacks are on the rise so improvements to cyber risk management and mitigation plans should be made now. With increasingly interconnected systems and exponentially growing quantities of data, industrial operations must put systems in place that allow them to detect vulnerabilities and respond when a breach occurs. Robust data and software system change management tools can help ensure companies remain running and prevent downtime during normal operations, and respond quickly and ensure resilient recovery when the worst happens.

About the Author

Jack Smith (jsmith@automation.com) is a contributing editor for Automation.com and ISA's InTech magazine. He spent more than 20 years working in industry—from electrical power generation to instrumentation and control, to automation, and from electronic communications to computers—and has been a trade journalist for 22 years.

About octoplant and AUVESY-MDT

octoplant is the first product jointly developed and brought onto the market since AUVESY merged with MDT. AUVESY-MDT provides manufacturer-independent version control and change management software. Its mission is to make automated production safer, minimize the damage caused by unplanned production downtime, simplify the lives of maintenance staff, and enable smooth collaboration.