TAG

WHY ACRONIS IS A LEADER FOR OPERATIONAL TECHNOLOGY (OT) CYBER RESILIENCE

DR. EDWARD AMOROSO,
CEO, TAG INFOSPHERE

Acronis

WHY ACRONIS IS A LEADER FOR OPERATIONAL TECHNOLOGY (OT) CYBER RESILIENCE

EDWARD AMOROSO, CEO, TAG

INTRODUCTION:

For decades, cybersecurity has been mostly synonymous with the protection of information technology (IT) from malicious attacks. Accordingly, Chief Information Security Officers (CISOs) have been put in place to guide this familiar focus. More recently, however, the scope of cybersecurity has been expanded to include more operation, industrial, physical, and tangible systems. The result is a new industry that we refer to as operational technology (OT) security.

Because OT security was developed in the wake of IT security, it shares many of the same types of controls. Creating visibility and deploying mitigation, for example, lie at the heart of both IT and OT security strategies – and this has been helpful as OT security continues to merge organizationally with broader IT initiatives. This is demonstrated by the many CISOs who are being given full OT security responsibility today.

As one might expect, however, many of the same weaknesses that exist in traditional IT security schemes will also be inherited for industrial protection. Perhaps the most obvious of such weaknesses is the typically fragile resilience many OT systems exhibit when under attack. Ransomware, for example, has been effective in bringing down large operational environments, leading to serious consequences for customers.

However, there are many unique problems that emerge in OT security contexts. These typically relate to the challenges of having no security-trained local staff in most OT environments, the plethora of older proprietary systems in place in these networks, and the often-challenging operational environments that make it especially difficult to perform updates or install patches without affecting the on-going mission of the environment (e.g., factory, manufacturing plant).

In this report, we explain how OT security teams, sometime now led by CISOs, can improve their operational resilience by focusing on one key function: Backup and recovery. This aspect of cyber protection has always been a challenge for IT security teams, because effective solutions demand intimate knowledge of the infrastructure, and most vendors working in this area have traditionally targeted IT operations rather than security.

For OT environments, we believe that backup and recovery are the most key elements in any initiative to improve security. Certainly, there must be complementary objectives to better train OT staff on security and to reduce the number of legacy systems in place. Our contention here, however, is that the biggest bang for the buck will come from OT security engineers focusing on this key element in the processing environment.

We will exemplify our discussion using the modern cyber resilience solutions from commercial vendor Acronis. Their approach to backup and recovery in any type of infrastructure, whether IT or OT, appears to be well-suited to the growing cyber threats targeting industrial operations in sectors such as manufacturing, transportation, energy, power, and military that cannot accept disruptions of any type.[1]

CURRENT SECURITY FOR OT SYSTEMS

As alluded to above, a major difference in the consequence of inadequate resilience between IT and OT infrastructure is that, in many cases, operational security issues can lead to more intense consequences. Resilience issues in industrial control, for example, could cause safety systems to fail, manufacturing lines to stop, or nuclear power plants to experience operational challenges. Scenarios involving the potential loss of human life are not hard to imagine.

This implies that security must be a high priority in OT environments. But these environments have been plagued by the challenges of heterogeneous and proprietary technology, often with obsolete hardware and operating systems. This limits the ability for patches and updates to be applied, not to mention the tight backup windows that exist in these environments, which are often not well-staffed with IT resources or trained experts.

Furthermore, the goal to isolate OT environments from hackers by inserting a gateway between IT and OT environments has not worked well. The original objective to hide OT systems from the Internet by creating an IT/OT perimeter has failed for all the reasons that perimeters always fail. They neglect to recognize insider threats, they miss access paths around the perimeter, they ignore the porous nature of any perimeter, and so on.

The IT/OT gateway approach also does not address the core OT security issues listed above related to proprietary systems, difficult patching, non-security-trained staff, and so on. The visual below shows how these security problems are not solved by an IT/OT gateway. It also does not address our main focus here – namely, OT security resilience requiring backup and restoration capabilities.

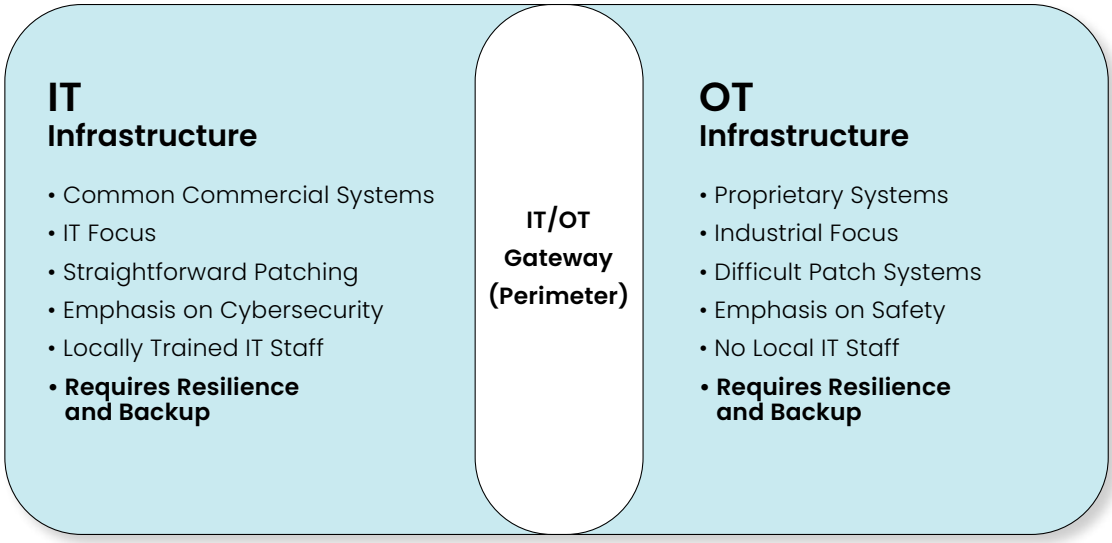

Figure 1. Security Challenges of OT Systems

As suggested, we understand that comprehensive OT security requires solutions to all of these problems. But we believe, and will explain below, that the assurance of on-going operations in the face of ransomware, sabotage, or destructive cyber-attacks must be the primary goal for modern OT security deployments. We will make this case in the context of the commercial Acronis platform and its support for OT security.

ACRONIS BACKUP AND RECOVERY SOLUTIONS FOR OT AND ICS

Our experience suggests that OT security programs must address three complementary areas. First, they should ensure visibility into the OT environment which they often obtain using commercial platforms such as Claroty and Dragos. Obtaining visibility is essential, and energy should be spent improving how it works in practice. This should include better training, and perhaps more emphasis on OT cyber range simulations.

Second, we believe that leadership should challenge their IT security teams to create more converged controls as OT systems integrate with IT. Trends in Zero Trust OT, for example, should be embraced, which implies that more operation systems connect with cloud and other traditional IT systems. This allows for extension of IT controls such as cloud native application protection platforms (CNAPP) to cover OT infrastructure.

But their third, and most importantly, we recommend that OT security teams begin to focus more on operational resilience. In practice, this implies the need to ensure continued operation through automated backup and recovery solutions. This obviously extends to IT systems as well, but as suggested above, disrupted OT support can lead to much more intense consequences, including for human safety – and the Acronis solution can help avoid these problems.

The security and resilience requirements most applicable to OT infrastructure are well-covered in the Acronis platform. This is good news, because enterprise teams should not have to develop their own local backup and recovery solution, even if their hardware and software are outdated and proprietary. Specifically, the key functions included in the Acronis suite that are essential for resilience in OT include the following:

1. **Rapid Recovery of OT Systems** – Acronis provides high-performance protection for OT computers, enabling swift restoration to prevent costly factory-floor outages. This rapid recovery capability is crucial in minimizing downtime and maintaining operational continuity.
2. **Universal Computer Recovery** – Acronis Cyber Protect ensures quick, reliable recovery for any computer, including older legacy systems that date back to the Windows XP era, with options for bare-metal restoration. This feature is essential for sustaining continuity with aging legacy systems common in OT environments.
3. **Customizable Backup Plans** – Acronis allows for the creation of customizable backup plans tailored to the specific requirements of OT and ICS environments, ensuring that critical data and systems are adequately protected. The need to customize is increasing as OT infrastructure modernizes using AI and more sustainable delivery methods.
4. **Integration with Third-Party Tools** – Acronis offers a unified backup and recovery view with centralized control and integration options into third-party tools, simplifying management and enhancing operational efficiency. OT environments are particularly challenging for security integration, so this capability is especially important.
5. **Data Sovereignty Options** – Organizations can choose between in-house storage or utilizing Acronis's global data centers, including options like Amazon S3 and Microsoft Azure, ensuring compliance with data sovereignty requirements. Acronis will work with customers to develop the most suitable hosting arrangement.

6. **Self-Service Recovery for Remote Workers** – Acronis provides self-service recovery options for remote workers, enabling non-technical personnel to initiate recovery processes, effectively decentralizing IT workload and accelerating the return to operation post-incident.

ACRONIS PLATFORM ARCHITECTURE

The Acronis Cyber Protect Platform is built around a data warehouse, which will store and secure the actual, historical, and other sources of key OT enterprise data. Multiple console instances of the Acronis Cyber Protect platform can be installed across the OT environment with associated multiple agents deployed across the environment for the purpose of data collection and restoration. Metadata is streamed from the consoles to the warehouse.

Dashboards and consoles for monitoring all aspects of the backup and recovery process are provided for each Cyber Protect deployment, as well as for the Acronis Centralized Monitoring Hub. This hub provides historical views, with customizable reporting and monitoring as the backup and recovery task is on-going. The purpose, obviously, is to ensure continued operation through incidents, attacks, and other resilience-related issues (see Figure 2).

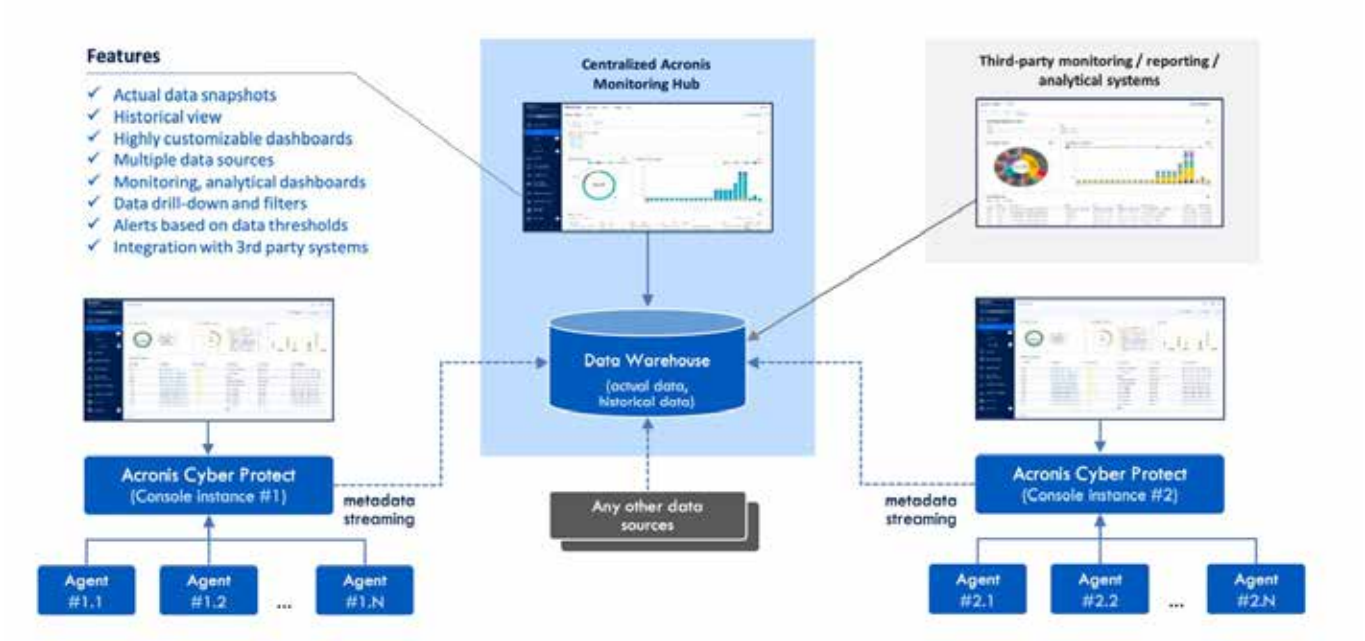

Figure 2. Acronis System Architecture

ACRONIS INTEGRATIONS

Acronis Cyber Protect (note the two instances depicted in the diagram) supports integration by unifying backup, disaster recovery, AI-based malware protection, remote assistance, and security tools into a single platform for the security team, including in OT. This consolidation allows any enterprise, and this includes OT security teams, to manage various aspects of cyber protection through one interface, reducing complexity and enhancing efficiency.

The platform's flexible architecture, application programming and command line interfaces supports the development and integration of third-party applications by both Acronis and third parties (note the third-party feeds depicted in Figure 2 connecting to the centralized data warehouse). This design promotes a dynamic ecosystem where additional protection, management, and automation

services can be incorporated, ensuring that the platform remains adaptable to evolving cybersecurity landscapes. This flexibility ensures that organizations can integrate Acronis's solutions into their existing infrastructures, enhancing overall resilience and security, especially in OT environments.

ACRONIS FORENSIC BACKUP

Acronis Cyber Protect includes a forensic backup feature designed to simplify future analysis by collecting digital evidence from disk-level backups. This capability is crucial for organizations that need to manage compliance requirements and conduct internal investigations efficiently. It is also essential for OT environments, where forensics can help to identify attacks targeting critical infrastructure and essential services.

The Acronis forensic backup process involves capturing comprehensive disk images, including active data, free space, and memory dumps. This thorough approach, which is increasingly emerging as an OT security requirement, ensures that all potential digital evidence is preserved properly, facilitating detailed post-incident analyses and supporting legal and regulatory obligations.

By integrating forensic data collection with regular backup routines, Acronis enables organizations in both IT and OT environments to maintain operational continuity while ensuring that critical forensic information is readily available when needed. This integration eliminates the need for separate forensic data collection processes, streamlining operations and reducing the risk of data loss during incidents.

ACRONIS INTEGRATED DISASTER RECOVERY

Acronis Cyber Protect offers an integrated disaster recovery solution that minimizes complexity while minimizing costs. By combining backup and disaster recovery capabilities, the platform ensures that businesses can quickly restore workloads after events such as natural disasters, human errors, cyberattacks, or hardware failures. As suggested above, these events in the context of OT systems can have serious consequences.

The disaster recovery features include the ability to quickly spin up IT or OT workloads in the event of a disaster, runbooks to automate recovery processes, and test failovers to ensure systems function as expected during an actual event. These capabilities are essential for maintaining business continuity and minimizing downtime, especially for real-time applications, so common in OT environments,

By integrating disaster recovery with cybersecurity and endpoint management, Acronis provides a holistic approach to cyber protection. This integration ensures that all aspects of an organization's IT infrastructure are safeguarded, promoting resilience against a wide range of potential disruptions. It also simplifies management for CISOs who have responsibility across both IT and OT production systems.

ALIGNMENT WITH REGULATORY REQUIREMENTS

In addition to the operational need for backup and resilience, OT security teams are increasingly being subjected to a variety of new external compliance and regulatory frameworks. The result is that OT cybersecurity compliance has become a much more challenging component of enterprise security programs, because it includes converged requirements that are evolving with increasing threats.

More specifically we see that global regulatory bodies are emphasizing operational resilience, through frameworks such as the Digital Operational Resilience Act (DORA) in the European Union and guidelines from the Basel Committee on Banking Supervision highlighting the need for robust cybersecurity measures in critical infrastructure sectors. Acronis's solutions support compliance with these regulatory requirements by providing support in the following areas:

1. **Comprehensive Risk Management Frameworks** – Acronis's solutions enable security organizations to implement adaptable risk management frameworks, regularly test resilience, and maintain open communication with stakeholders and regulators, aligning with global operational resilience frameworks for both IT and OT.
2. **Incident Response Planning** – Acronis assists in developing written incident response plans, either standalone or as part of a business continuity plan, ensuring preparedness for potential cyber threats. This is a new task for many OT security teams, so the support from Acronis is especially helpful here.
3. **Third-Party Risk Management** – Acronis's integration capabilities facilitate robust third-party oversight, a critical component of operational resilience as highlighted by regulatory bodies. As suggested earlier, cyber integration with third parties can be challenging because it has previously been either ignored or de-emphasized.

LEADING OT AND ICS AUTOMATION VENDORS RELY ON ACRONIS

The adoption of Acronis backup and recovery solutions by the world's largest OT and ICS platform vendors underscores its critical role in ensuring resilience within OT and industrial environments. Industry leaders such as ABB, Emerson, Siemens, Schneider Electric, Rockwell Automation, and Yokogawa integrate Acronis Cyber Protect into their platforms—either as a white-labeled or co-branded solution—delivering operational resilience to their customers. The fact that these global giants have standardized on Acronis speaks to the platform's reliability, flexibility, and leadership position within OT backup and recovery.

CONCLUSION AND ACTION PLAN FOR OT SECURITY TEAMS

We believe that Acronis's backup and recovery solutions are well-suited for customers seeking to enhance resilience and security in their OT infrastructure. By offering rapid recovery capabilities, support for legacy systems, customizable backup plans, and alignment with regulatory requirements, Acronis enables organizations to maintain operational continuity and comply with evolving global standards in operational resilience.

Our advice would be for CISOs tasked with this responsibility, or any other management or leadership team working to address cyber resilience for OT, to immediately engage with Acronis to learn more about their capability. Our team at TAG is also available any time for readers to leverage in their efforts to develop deeper insights into this and related topics in cybersecurity and artificial intelligence. We look forward to hearing from you.

[1] We are especially grateful to the Acronis technical and leadership teams for helping us understand the various risks they are seeing in OT environments operated by their clients. The Acronis team gave us access to their product documentation and helped us gain useful insights into their product roadmaps for both IT and OT security.

ABOUT TAG

TAG is a trusted research and advisory company that provides insights and recommendations in cybersecurity, artificial intelligence, and climate science to thousands of commercial solution providers and Fortune 500 enterprises. Founded in 2016 and headquartered in New York City, TAG bucks the trend of pay-for-play research by offering unbiased and in-depth guidance, market analysis, project consulting, and personalized content—all from a practitioner perspective.