The day after

Recovery, resistance and resilience after an industrial cyber-attack

In today's alarming reality, adequate ransomware response and recovery programs should be embraced as crucial business enablers. Improvising when an organization's OT and critical operations are engulfed in a deadly firestorm is likely not the answer.

In the case of a large oil pipeline system, a major ransomware attack caused a shutdown of operations for almost one week and led to fuel shortages. The attack — the result of a single compromised password — focused on the pipeline's IT systems, but the operational technology (OT) systems that transport oil were not directly targeted. The attackers stole data and infected the IT network with ransomware and to prevent it from spreading to the OT, the pipeline was shut down.

Ransomware attacks, which spread across the network and encrypt data, are soaring worldwide. Decryption of business data can be almost impossible amid today's increasingly sophisticated ransomware attacks, during which attackers typically demand a ransom payment in bitcoins to release a key for data decryption. The organization under attack must either pay to regain access to its data or hope to recover the data in some other way, such as via backup applications.

As ransomware attacks skyrocket, ransoms could cost businesses a total of US$265 billion by 2031, according to Cybersecurity Ventures, which predicts costs will rise by 30 percent annually over the next 10 years.[1]

Effectively managing an attack is critical in order to address the initial impact on operations and costs, and to help minimize a recovery that may involve days or weeks of limited capabilities and interrupted customer services. Businesses need to prepare not only for an attack response but for rapid recovery — and this is particularly critical in the OT domain, where physical processes are typically involved. While many businesses are racing to enhance prevention and response programs, they also need appropriate recovery capabilities.

Recovery measures to restore operations quickly require a precise assessment to determine that the initial underlying threat has been eliminated. This is no small task amid the immediate need for response measures that include shutting down internal systems and key elements of the business network, along with rushed policy changes.

It's also crucial that the complex path back to normal operations includes key changes to security. The response and recovery process under these typical conditions can create remarkably complex challenges.

What's operational technology?

Operational technology (OT) involves the use of hardware and software to control industrial equipment. OT security is becoming vital today as OT is integrated with IT to create IT/OT convergence. Because IT and OT networks can no longer be separated, attacks on IT affect OT and vice versa.

This offers attackers a wider attack surface and makes a comprehensive security approach crucial. However, this is currently not being prioritized as it should be by businesses and OT is increasingly being targeted by disruptive attacks.

[1] David Braue, "Global ransomware damage costs predicted to exceed $265 billion by 2031," Cybersecurity Ventures, June 2, 2022.

Modern OT security is now the cost of doing business

Investing in appropriate protection is the cost of doing business today. It's important to understand how connected IT and OT machines and applications communicate, the state of their network segmentation, and current risks as ransomware attacks soar.

While IT is the technology backbone of any organization, businesses engaged in manufacturing, mining, oil and gas, utilities and transportation rely heavily on OT to connect, monitor, manage and secure their industrial operations. And though OT is typically associated with industrial operations, other sectors pursue efficiencies through OT, such as e-commerce giants relying on automated warehouses and digitally connected operations.

You may have OT assets in your organization even though it is not OT driven. Medical devices, warehouse automation, smart-building appliances and large air-conditioning systems are OT that could be affected in an attack. The sooner you identify and understand the significance of OT systems in your organization, the sooner you can enhance your cyber resilience.

Threats to critical infrastructure and public safety are rising

While IT disruptions and compromises can have obvious widespread impacts affecting consumer services, data security and public safety, ransomware attacks disrupting critical-infrastructure OT systems can also create havoc and threats to the public.

For example, an attack that disables a major electrical utility can have serious implications for public safety amid the lack of critical services, making rapid recovery paramount. Consider the debilitating public impact of an attack that disrupts public water services for days or weeks. The nature and impacts of today's cyber-attacks are increasingly broad and can pose — beyond impacts to manufacturing supply chains providing essential consumer products — a threat to public ecosystems serving massive geographies and populations.

A good example is the 2017 WannaCry attack that infected computers in more than 150 countries. One of the largest ransomware attacks to date, it disrupted health services, telecoms and transportation. The toll on public services and safety was unprecedented.[2]

While businesses may rely on a single primary IT provider, those same businesses could depend on 10 or 20 interconnected OT system providers, making recovery complex — and requiring specific recovery expertise — in an attack involving sophisticated techniques.

Beware — a ransom payment can guarantee nothing

The recovery process to restore and operationalize normal activity typically requires updating — or rebuilding from scratch — disrupted databases, business systems and operations. There is a high probability that even if a ransom is paid, or a business recovers encrypted data without a payout, segments of the business will face a costly and time-consuming rebuild requiring months to complete.

Unfortunately, businesses often mistakenly assume that operations are immediately restored if they pay the ransom and obtain the recovery key to decrypt data.

A comprehensive analysis of how the breach occurred — and identification of security gaps — is crucial to enhancing OT safeguards and helping to minimize future risk. In most cases, businesses possess adequate business-continuity and disaster-recovery plans to cover conventional risks such as technical failures or natural disasters. But they may lack a comprehensive — and continually updated — playbook addressing the devastating disruption at risk in a ransomware attack.

Success fending off an attack today does not guarantee success tomorrow. OT vulnerabilities and attack surfaces change and multiply as businesses 'drift' or evolve. Testing of playbooks and recovery simulations is therefore critical.

For most executives, a ransomware attack simulation is often an eye-opening event, revealing both a lack of OT safeguards and gaps that can impede recovery. Leaders huddled in a simulation war room may be flying blind as they suddenly realize that they cannot quickly identify the impact of an attack or manage extreme scenarios.

The first 72 hours are critical to recovery

KPMG firms have witnessed a lack of robust planning and OT backup capabilities — and the costly impact on recovery time. The need for speed during recovery is instrumental. But too many organizations wrongly assume that recovery will require several weeks to return to business as usual — instead of several months or more. The result is typically a slow response in identifying an actual attack, the business assets and operations impacted, and the sequence of events that needs to unfold without delay.

When an attack strikes, the initial 72 hours are critical but never easy for typically panic-stricken leaders suddenly engulfed in a catastrophic scenario demanding negotiation with an organized crime group while attempting to grasp the scope of the attack.

[2] Jennifer Gregory, "WannaCry: How the Widespread Ransomware Changed Cybersecurity," Security Intelligence, October 30, 2020.

The need for well-structured OT recovery programs has become indispensable, taking in the entire ecosystem in terms of critical processes and assets, support and backup capabilities, and the sequence needed to rapidly restore operations. Roles and responsibilities should be clearly defined. A plan for communications to all stakeholders is also imperative.

Businesses need to understand that OT recovery poses unique challenges that should be addressed early and according to conditions that vary across industries. Simply halting systems or disconnecting elements of the business network is not always possible within OT, given that it may control critical systems and sensitive physical processes.

An overly simplistic approach of resorting to manual operation during a crisis may prove impossible for many reasons. For example, digitally automated product warehouses probably lack personnel for manual delivery. In the case of an electrical distributor, the organization may lack personnel skilled in manual operations.

Rapid recovery demands close collaboration

In recovery mode, cybersecurity specialists should engage with OT specialists early on to craft specific scenarios and leverage existing plans. At the same time, OT engineers and administrators will likely have protocols for other types of disaster scenarios that can support response and recovery efforts.

Initially, consider classifying the incident and reviewing procedures and your response checklist, helping to ensure alignment with best practices and the organization's structure. This includes technologies and tools in place and those that others can provide.

With this information compiled, identify key stakeholders impacted and the 'chain of custody' — the digital and physical evidence related to the attack. For those involved in the chain of custody, due diligence in collecting digital evidence is critical to avoid compromising evidence. KPMG's well-established recovery approach is structured in five phases.

Phase 1: Respond | Steps to respond to a cyber event

- Don't panic and keep a cool mind.
- Identify and analyze the threat.
- Report the incident.

Phase 2: Remediate | Steps to remediate root cause

- Contain and eradicate the threat.
- Make a detailed record of the attack.

Phase 3.1: Tactical recovery phase | Steps to recover from an attack

- Determine the impact of the cyber event.
- Identify the adversary's footprint on the infrastructure, command and control channels, and tools and techniques.
- Use all available information gathered to create the restoration plan.
- Begin to execute restoration by validating and implementing remediation countermeasures in coordination with the incident response team and other information security personnel.
- Document any issues that arise, any indicators of compromise, and newly identified dependencies.

Phase 3.2: Strategic recovery phase | Steps to recover from an attack

- Develop a plan to correct the root cause of the cyber event.
- Implement changes to strengthen the security posture of the organization.
- After recovery is completed, review metrics that were collected.

Phase 4: Resistance | Enhance posture to resist a future attack

- Prioritize capabilities to enhance the cyber posture.
- Develop a pragmatic design and plan to implement.
- Programmatically implement capabilities.
- Validate effectiveness with regulatory-level testing.

Phase 5: Resilience | Maintain discipline to remain resilient to an attack

- Establish a tool-informed solution and team to monitor drift from policy.
- Aggregate and analyze signals to identify issues.
- Prioritize issues and integrate them with existing remediation processes.
- Track remediation to completion and report executive scorecards.

There are different approaches to help prepare against attacks. Potential activities are clustered into three categories, and we recommend focusing on *reactive* activities.

After a successful attack, it's important to initiate countermeasures and contain the attack. In our experience, it is never possible to discover and eliminate all weak points beforehand. If an attack occurs, you must eliminate the danger. That's why our recovery approach is part of the reactive activities:

Preventive	Proactive	Reactive
Prevent attacks, minimize attack surface	**Take steps to make an attack less severe**	**Run through scenarios of a successful attack**

Recovery capabilities are lacking as threats soar

Businesses are making good progress developing more appropriate *response* capabilities. But beware — appropriate *recovery* capabilities continue to show room for improvement. In our view, typical business-continuity planning is not keeping pace with the changing cyber environment. Businesses should start thinking differently to understand the critical path needed for effective recovery.

Organizations should start planning for a worst-case scenario that poses a potentially existential threat to the organization. In addition, be prepared with a support team that can come in and provide disaster recovery at a moment's notice. Numerous businesses are providing outsourced cyber-response capabilities, but very few deliver cyber-recovery capabilities and skills aligned to today's threat environment.

Finally, it's crucial to test recovery capabilities regularly. Having a disaster-recovery plan and resilience in place without comprehensive testing isn't a recommended way to approach today's threats.

There is little time to lose as the frequency and impact of attacks grow

These are unique business challenges today. Racing for solutions when an organization has been paralyzed and the clock is ticking on an existential threat to the business is not your typical CEO challenge.

Business leaders need to be champions of change and show a sense of urgency in promoting OT response strategies, smart playbooks and recovery mechanisms. With ransomware attacks soaring, the capability to respond and recover quickly should be seen as a competitive advantage.

Unfortunately, many organizations believe they will be spared from a ransomware attack and they continue to dedicate inadequate resources and investment to the problem.

Forward-looking businesses are raising their game. And there is little time to lose as cybercriminals continue to do the same with increasingly lucrative ransomware schemes. Innovative businesses assessing today's profound OT threats are thinking *when*, not *if*.

[2] "Executive Order 14028, Improving the Nation's Cybersecurity", NIST. (November 8, 2021)

OT recovery readiness — being prepared for anything

When there's a disaster, production outage, ransomware attack or other event, you need to get your OT and production processes back online quickly. That means always being ready for anything. And given the constant change in today's OT environments, ransomware readiness can't be something you address quarterly or annually. Readiness should be a daily focus.

The constantly growing and changing scope of threats should always be taken into account. It's not only about on-premises systems, but also IT and OT systems and their connected OT components such as the control system and programmable logic controllers (PLCs).

You need the capabilities to recover modern and old production systems, virtual machines (VMs), containers, programmable logic controllers (PLCs) and applications from anywhere in a modern hybrid IT/OT architecture. The cloud has also become part of today's modern systems or OT infrastructures and these platforms also need to be considered.

This complexity clearly shows that one-size-fits-all approaches are usually unsuitable for OT and production sites at this point. To be prepared for an emergency, the following key points of recovery readiness should be achieved in order to restore operations within a reasonable time frame:

First, be aware of all your critical assets for IT and OT and their dependencies on each other. Also maintain up-to-date vulnerability reports from your critical systems and assess them on a regular basis. Without this kind of information, we believe recovery in a tolerable time frame is impossible.

Define recovery objectives when recovering from a disruption. For example, the recovery capability should prioritize human and environmental safety prior to restarting the OT operation that was impaired by the cybersecurity event.

Develop a site disaster-recovery plan (DRP) and business-continuity plan (BCP), or both, to prepare the IT and OT organization to respond appropriately to significant disruption during a cybersecurity incident. It's important that IT and OT are not considered separately but together (IT/OT convergence goal).

Establish backup systems and processes to back up the relevant (critical) OT systems' state (legacy systems, Windows/Un ix, PLCs, virtual systems etc.), data, configuration files, and programs to support timely recovery to a stable state.

Create awareness of threats (not only for IT), train your OT employees, simulate the worst-case scenario and learn from your findings.

If you have not yet implemented these points, you should do so as soon as possible in view of the current and constantly increasing OT threat environment. We recommend focusing on your critical OT systems in the first wave of recovery readiness, followed by the medium critical and less critical in waves two and three.

Contributors

Thank you to the following people for their support and contributions to this article:

Walter Risi (Global Lead for IIoT Cyber Security Services, KPMG International), Jason Haward-Grau (Global Cyber Recovery Services Leader, KPMG International), Pablo Almada (Partner, Cyber Security Services, KPMG in Argentina), Hossain Alshedoki (Associate Director, IT/OT Cybersecurity & Data Privacy ENR Lead, KPMG in Saudi Arabia), Thomas Gronenwald (Senior Manager, Head of Industrial Cyber Security, KPMG in Germany, Florian Thiessenhusen (Senior Manager, Cyber Security Services, KPMG in Germany).

For more information contact:

Walter Risi
Partner, KPMG in Argentina and
Global Lead for IIoT Cybersecurity
KPMG International

E: wrisi@kpmg.com.ar

Marko Vogel
Partner,
KPMG in Germany

E: mvogel@kpmg.com

Jason Haward-Grau
Principal,
KPMG in the US and Global Cyber
Recovery Services Leader
KPMG International

E: jhawardgrau@kpmg.com

Designed by Evalueserve.
Publication name: The day after | Publication number: 138514-G | Publication date: December 2022