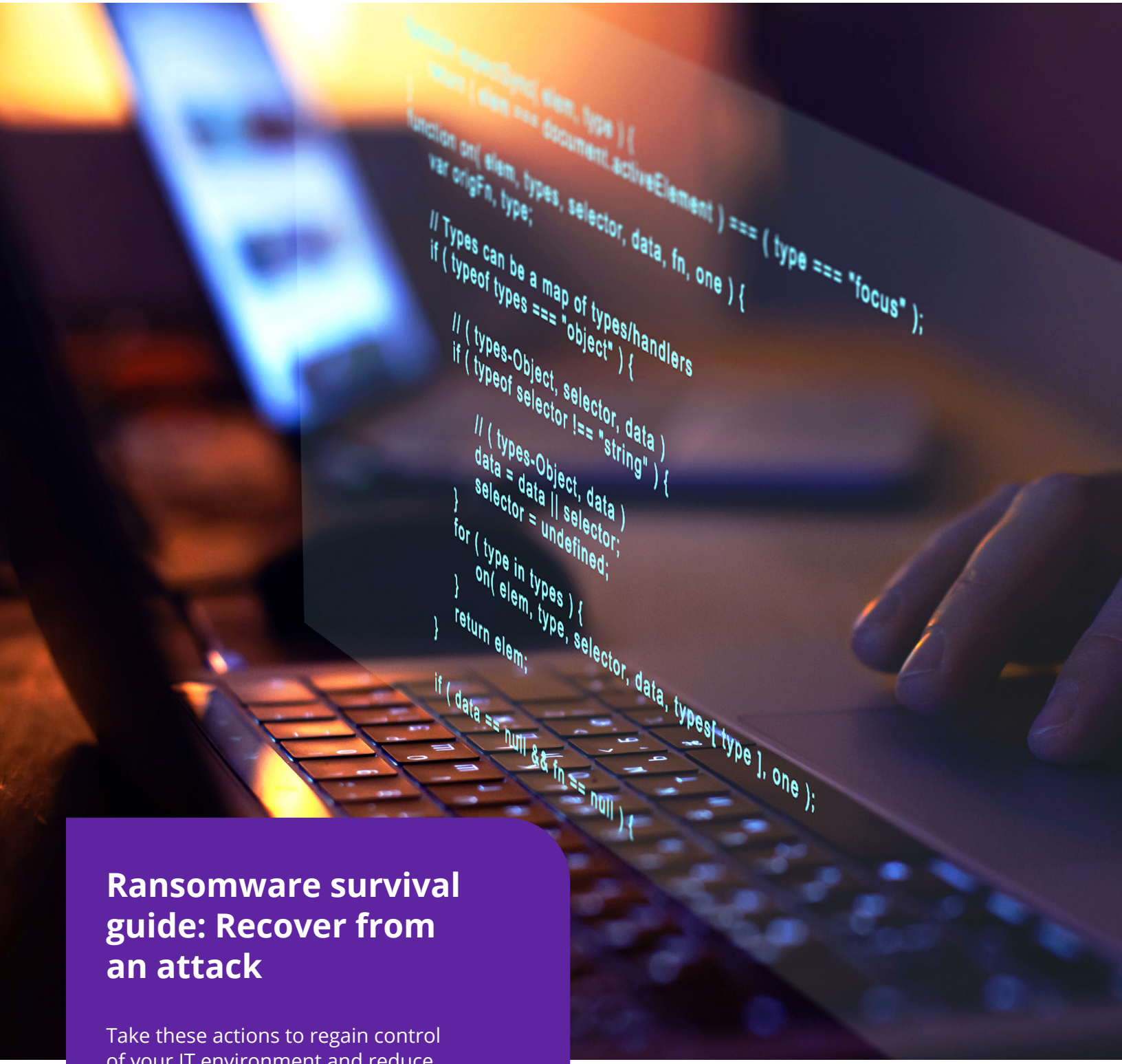
DXC TECHNOLOGY



Ransomware survival guide: Recover from an attack

Take these actions to regain control of your IT environment and reduce business impact

Table of contents

The impact of ransomware attacks

Ransomware attacks are an unwelcome and increasingly concerning but unavoidable fact of life today. Industry experts estimate that by 2025,[1] 75 percent of organizations will have faced one or more attacks, incurring an average of $1.85 million in recovery costs[2] along with potentially grave damage such as interruption of essential services.

Criminal groups are now offering ransomware as a service to distribute tools and tactics to a growing cadre of affiliates — and many attacks have expanded beyond attempts to encrypt data and render systems unusable. Sophisticated threat actors are now exfiltrating data and threatening to publish it, sell compromised credentials or delete an organization's data altogether. Ransomware has become a lucrative activity, with businesses and government agencies making $5.2 billion in bitcoin ransom payments since 2018.[3]

In a ransomware attack, the ideal scenario is to hold the attacker at bay while security and IT teams work to contain, analyze and recover from the attack. Invariably, however, the question of ransom payments surfaces. DXC advises organizations not to pay a ransom — not only because of the potential ethical and legal implications but also because payment does not guarantee a safe or complete recovery. It has been demonstrated that organizations that pay ransoms on average can only restore 65 percent of their data.[4] Worse than this, some organizations have been recompromised due to failing to identify root causes and securing their networks.

As one of the world's leading security services providers, DXC has helped many global companies and public sector agencies recover from ransomware attacks. We also work with customers to harden their environments against the latest tactics and techniques of threat actors.

In this ransomware survival guide, we share lessons we've learned and best practices we've developed to help organizations coordinate their response to an attack and make timely, strategic decisions through all phases of the response. This guide is a follow-up to DXC's Ransomware defense guide: Prepare for an attack, which focuses on proactive attack prevention. The defense guide includes a checklist to help organizations identify weaknesses in their environments that could be exploited, reduce attack surfaces and lower the likelihood of successful attacks.

1 "Detect, Protect, Recover: How Modern Backup Applications Can Protect You from Ransomware," Gartner, January 2021.

2 "The State of Ransomware 2021," Sophos, April 2021.

3 "Ransomware Trends in Bank Secrecy Act Data," U.S. Treasury, Financial Crimes Division, Oct. 15, 2021.

4 The State of Ransomware 2021," Sophos, April 2021.

Life cycle of a ransomware attack

Many adversaries plan for weeks or even months before launching the actual attack. For the attacked organization, the full recovery process can take up to a year. DXC has developed a model of a ransomware attack that includes both the phases of the attack and the response. (**Figure 1**).

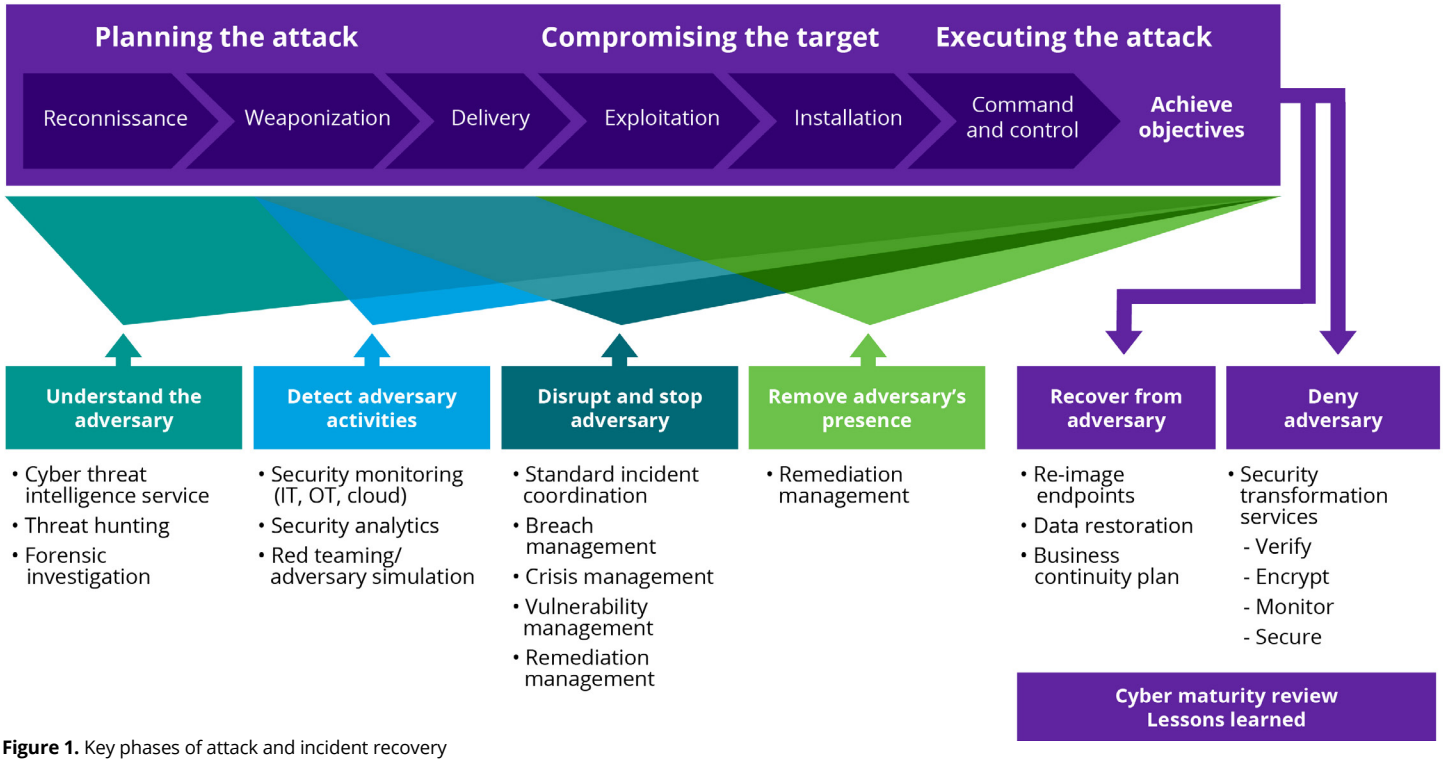


Figure 1. Key phases of attack and incident recovery

The model helps us to map the activities to the phases of the activities and can be adapted or enhanced with industry frameworks such as MITRE ATT&CK or NIST IR guides.

The order of the phases shown in Figure 1 is aligned with the preventive approach described in our ransomware defense guide; however, in the event of a ransomware breach where detection has already occurred, the top priority should be disrupting the attack.

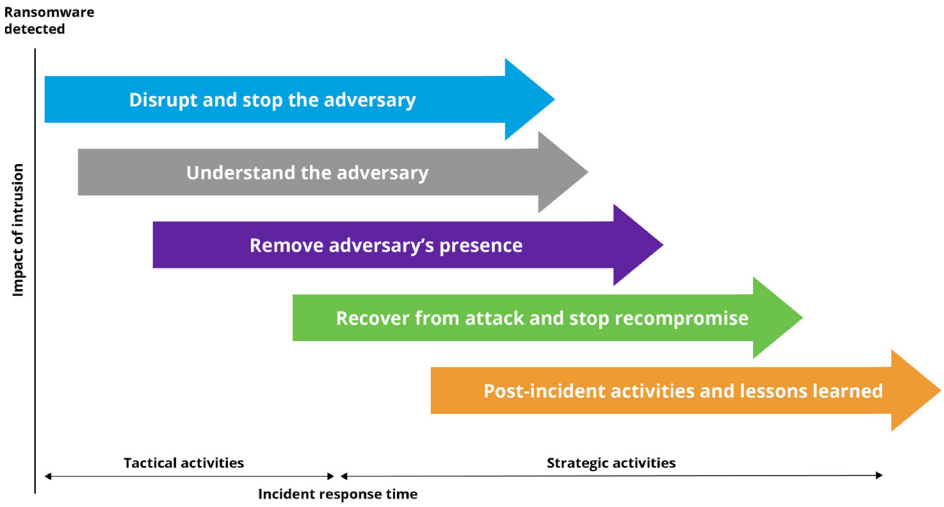
Therefore, this guide focuses on the following activities, in five phases:

- Disrupt and stop the adversary
- Understand the adversary
- Remove the adversary's presence
- Recover from the attack and avoid recompromise
- Perform post-incident activities and lessons learned

While this report is organized in five phases, it's important to note that remediation activities generally need to be done in parallel. **Figure 2** shows how these phases overlap.

This overlap creates staffing challenges, as key personnel are often involved in multiple activities. The ability to prioritize effectively in the face of unknown elements is key to surviving a ransomware attack.

Figure 2. Phase overlap



The task of beginning the recovery and remediation process can be daunting. To help address this need, DXC has created a comprehensive blueprint that groups the commonly required activities into 180 pages of work packages (**Figure 3**) based on our proprietary Cyber Reference Architecture and informed by our work with large global organizations.

This matrix helps prioritize activities based on an organization's cyber-maturity level and capabilities.

Although the structure shown in Figure 3 is similar to that in the National Institute of Standards and Technology's Computer Security Incident Handling Guide, [5] it's shaped by our real-world experience.

Clearly, dealing with the aftermath of a ransomware attack is a complex task. In addition to the security-centric tasks shown in Figure 3, the response must entail a wide range of tasks related to external and internal communications, access control systems, business solutions, operational technologies (OTs) and many more potential issues specific to impacted systems and infrastructure.

5 "Computer Security Incident Handling Guide," National Institute of Standards and Technology, U.S. Department of Commerce, August 2012.

Recovery and remediation blueprint

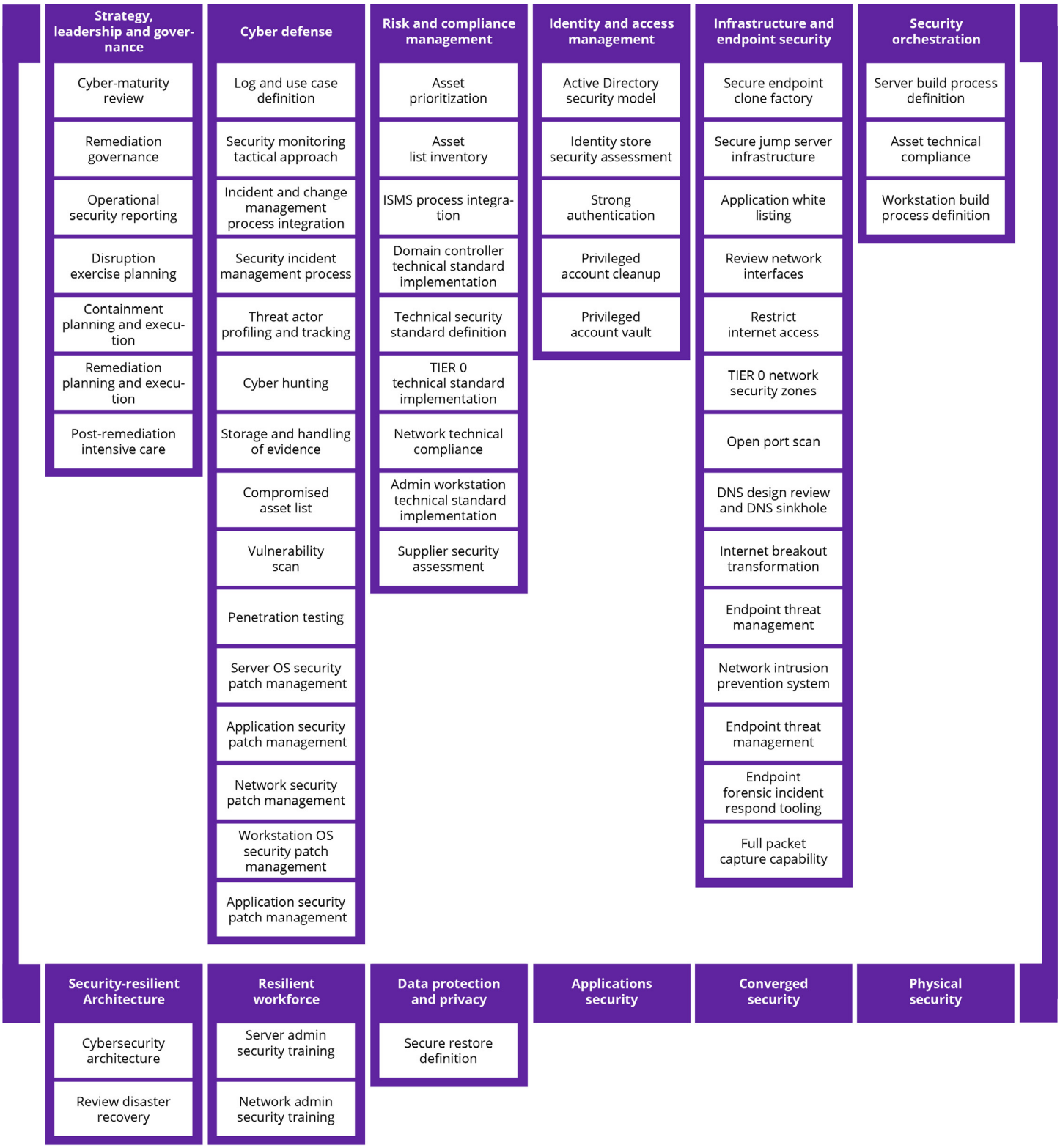


Figure 3. Remediation blueprint work packages across security domains

Effective action results only from effective coordination and control, which requires strong governance and highly organized recovery efforts. Typical roles and functions involved in a ransomware crisis are illustrated in **Figure 4**.

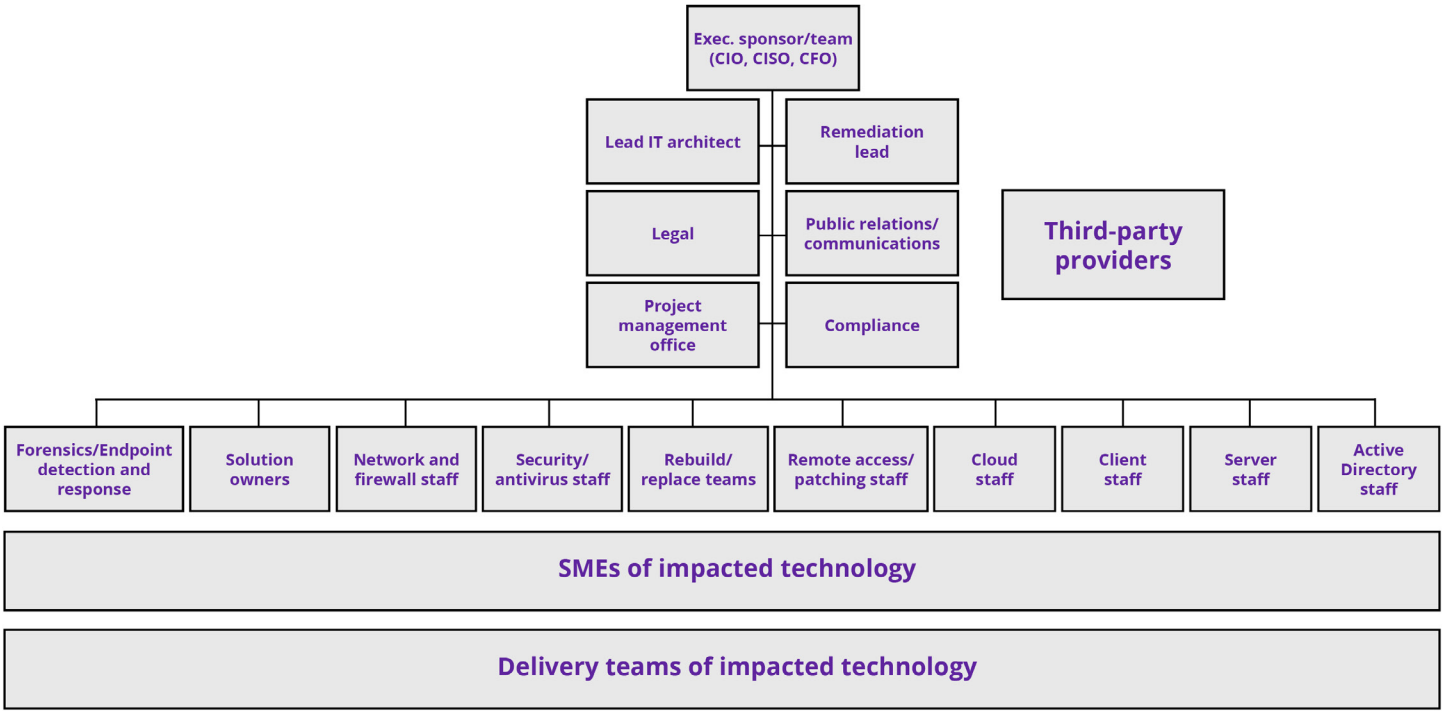


Figure 4. Typical incident response roles and functions involved in a ransomware attack

Ransomware attack scenario

The remainder of this paper brings the model to life.

In the following scenario, the attack begins on a Friday evening. The IT help desk begins receiving reports from around the world of a ransomware message screen and services that are no longer functioning correctly.

The victim is a global company that has many of the capabilities required to respond effectively but lacks proper preparation. Its incident response teams include more than 250 people from all regions and all technical domains, from administrative to senior leaders, working 24x7 and in shifts. Rather than suffering fast, widespread impact and encryption by the perpetrator, the strike's impact on this company is slower and less pervasive because security preparedness has limited the impact. There is still a chance to protect some resources and further reduce the impact if the organization reacts efficiently. The encryption process has begun, but it is occurring slowly and has affected only a few random systems.

Let's discuss the key measures that other organizations can take to respond to a ransomware incident like this.

1. Disrupt and stop the adversary

The organization's first priority is to ensure that the ransomware does not spread further within the environment.

The remainder of this section deals with two major topics – gaining visibility and forensic analysis. It's worth noting that at this point in the response, senior management should ensure that governance and control mechanisms are established to manage many activities, including tracking the costs incurred by the incident.

1.1. Containment activities and visibility

In this phase, the adversary's ability to move around in the environment is blocked. The activities are informed by findings from digital forensics activities.

- Secure crown jewels and crucial systems (agree on priority systems and services)
- Block network traffic
- Isolate network segments
- Block malicious/suspicious domains and emails
- Reset passwords for and reduce the number of privileged accounts
- Restrict highly privileged accounts where required
- Isolate known compromised hosts
- Monitor for indicators of compromise
- Collect malware sample and organize custom DAT file from antivirus vendor

Additionally, a key activity in this phase is to get the best possible overview of the current situation. Anything learned can help management and response teams make more informed decisions for the activities to come. Increased visibility into the situation helps teams define configurations and tooling in later phases to better protect and more quickly clean or rebuild the impacted environment.

75%

share of organizations that will face one or more ransomware attacks by 2025

$1.85M

average cost of recovery from a "ransomware attack

Forensic services will lead efforts to find indicators of compromise, which will increase visibility and help the remediation team disrupt the adversary. Most of these activities follow each other closely, with focused switching from one phase to the other, while a low level of constant activities is performed continuously in the background.

Concurrently, organizations must re-enable impacted systems and services, analyze how the environment was compromised, improve visibility into the incident, and plan and configure improvements that block the threat actor's ability to recompromise the environment.

Required information includes:

- Where did the incident start?
- Who detected the event and how?
- Which systems, users and services are impacted?
- Prioritize recovery activities based on business impact, with attention to crucial services and related dependencies to other services and infrastructure
- Are people's health or lives at risk? Has the threat been mitigated?
- Are any countermeasures already applied? If so, what measures were taken? When and where?
- Can system elements be separated, such as blocking rules on routers and firewalls and pulling virtual network cables?
- Are IT and OT systems separated? If not, can they be? What are the dependencies between them?
- Does remote access still work?
- Has any suspicious activity been observed, such as account activity associated with privileged identities or password resets?
- Are log files available from suspicious systems?

Another important question to be answered is: Are backups secured, isolated, accessible and/or recoverable? Backups should be offline and encrypted, with access restricted, and organizations should conduct regular training and exercise to ensure they are recoverable in case of an incident. An air-gapped vault solution is one useful approach.

After the initial fact-finding phase, the organization and supporting vendors need to come together as soon as possible to plan and push for further enhancement and execution of governance responsibilities. The response must be organized and communicated to all stakeholders, including legal, management, IT and staff. Additionally, management should declare a crisis and initiate the relevant crisis management and communication processes, including standing up the relevant response organization (**Figure 4**).

DXC advises organizations not to pay a ransom — not only because of the potential ethical and legal implications but also because payment does not guarantee a safe or complete recovery.

2. Understand your adversary

The main goals of forensic analysis are to understand how the malicious code came into the environment and isolate the affected devices from the network as quickly as possible to prevent encryption of mapped network drives and other systems.

Indicators of compromise collected during this analysis will help the teams articulate the necessary countermeasures and prioritize their remediation work based on the tactics, tools and procedures of the threat actor and the breadth of the compromise.

The following forensic activities are typically required:

- Recommendations on **visibility tools, deployment and placement** (the typical minimum threshold for visibility is 80 percent)
- **Forensic analysis** of compromised systems, accounts, services, files, storage, memory, command and control channels, malware type analysis, reverse engineering, etc.
- **Malware analysis**, a complex and difficult exercise made even more challenging by threat actors' attempts to hide their persistence and encrypt malicious payloads
- Collecting **indicators of compromise and defining countermeasures** and containment tools such as firewall blocks and sinkhole configurations, custom antivirus signatures, file blocks, software updates, component deactivation, etc.
- Support during the **creation of cleaning strategies and rebuild** approaches
- Participation in calls with **cyber insurance organizations** and other third parties

3. Remove the adversary's presence

After the immediate threat has been contained and encryption largely stopped, the work begins on removing the adversary from the environment.

This phase often starts in parallel with disrupting the adversary, with the degree of overlap driven by a number of factors including the organization's overall risk tolerance — balancing the need to restore critical business processes with the risk of recompromise.

If the organization has been prepared for a crisis situation such as a ransomware attack, the organization can respond significantly faster and more effectively. Key steps are time-consuming activities such as:

Organizational

- Synchronization and approval with various groups
- Definition of "crown jewels" and essential business services

Technical

- Definition of high-value target systems such as domain controllers ADFS, PKI, AADsync, etc.
- All cyber defense activities (referenced in the Ransomware defense guide)

Organizations often need to prioritize restoring core identity functions such as Active Directory and DNS so they can begin the wider recovery.

Technical workstreams required for recovery will depend on what was impacted by the attack.

Governance and control continue to accelerate in this threat actor removal phase. Communications with customers and partners will become more intense, and questions are likely to move from "What is happening?" to "Why did it happen?" and "Wow, can we trust you?"

It is essential to actively monitor for potential suspicious activities and continuously update the tooling with information from the forensic investigation.

Typically, authorities are notified in this phase, and communications teams prepare internal and external announcements.

The overall volume of activity and related interactions rises with a corresponding demand for management input. A project management framework must be put in place at this point to address the complexity of technical tasks.

For most organizations, recovery will impose a significant load on subject matter experts, and success requires a structured approach to managing priorities. Business impact and continuity should be addressed with analysis of non-IT related and IT-dependent service issues.

3.1. Cyber security insurance

A growing number of organizations have purchased cyber security insurance coverage to recover costs; therefore, forensic teams need to meet insurers' requirements for documentation and execution of incident response activities.

Often these tasks must be approved or at least synchronized according to insurance policy requirements.

Third-party service providers such as DXC should participate in discussions with insurers to explain initial findings and how to respond to the incident.

4. Recover from the attack and avoid recompromise

The most comprehensive and secure approach to recovery is to assume widespread impact of the malware and rebuild from scratch. But often this is not practical or possible.

The clean-and-rebuild program includes a general set of activities that are more or less the same for all servers and clients independent of their specific role, plus a set of role-specific activities that are unique to the particular server, role, software, solution or product.

Isolate but don't shut down suspicious machines, so you don't lose any important forensic data that is only stored in memory.

Typical activities that are common across a broad range of products and server roles include:

- Rebuild and clean the hardware-adjacent software and components such as BIOS, drivers, etc. Make sure you have a trustworthy software library and verified software hashes.
- Rebuild and clean the memory, operating system and registry. Ensure that you have scanned the server with an antivirus and/or endpoint detection and response tool that can detect the malware found during analysis.
- Harden the server following vendor recommendations.
- Perform credential hygiene following recommended practices:
    - For service accounts, allow "logon as a service" and "logon as a batch job." Deny "logon locally" and "logon through remote desktop services" and make sure they are not allowed for interactive logon.
    - Define a secure management client (secure admin client) that is exclusively able to access high-security systems.

65%

amount of data, on average, that companies are able to restore after paying a ransom

$5.2B

estimated ransom payments made in bitcoin since 2018

Apply known good configuration settings that have been defined for the incident, such as:

- Custom antivirus pattern with the latest version
- Endpoint detection and response tools and agent installed
- Patch level and latest patches installed
- Privileged accounts reset
- Negative antivirus and endpoint detection and response scan results
- Participation in monitoring
- No other signs of malicious activity

During all of these activities, it is essential to actively monitor for potential suspicious activities and continuously update the tooling with information from the forensic investigation.

The most common activities to clean, rebuild and secure servers and clients as well as related assets (such as accounts, applications, etc.) are listed in the work packages shown in Figure 2 (remediation work package prioritization).

After the general base hardening, role-specific hardening and clean-up/rebuild should begin. The organization must decide whether to rebuild or clean a system based on the findings, availability of backups, complexity of rebuild, the overall risk appetite and the specific situation. Business dynamics can have a significant influence in these decisions and parameters. For example, the need to close year-end financials may put significant pressure on decision makers and influence the approach and priorities.

One of the most important requirements of the remediation phase is having a good understanding of the Active Directory design, domain model, trusts and the way the environment is accessed. Key areas of concern are remote access entry points, location type and patch level of security boundary devices, as these access points are regularly compromised by threat actors.

Rebuild-and-clean teams also should review all privileged groups and strictly apply the least-privilege principle, remove members from groups such as enterprise admins or schema admins, and apply permissions only for the time required for administrative tasks. Use multifactor authentication for least-privileged access and apply strict monitoring for relevant entities.

Planning needs to take into account the time required to implement improvements and see benefits. Sometimes it can be faster to implement a tactical change to achieve some benefit, knowing that strategically this approach will need to be enhanced or replaced. Ideally the approach should support both short-term tactical and long-term strategic requirements.

When rebuilding servers, the time required to restore data can vary from several hours to several days based on system complexity and the nature and amount of data.

Experience shows that investing in prevention and protection before an incident occurs is significantly easier and less expensive than conducting recovery and clean-up under attack conditions. Even better, organizations can avoid potential business interruption and reputational damages.

Backups often must be restarted because the data is unusable. A trained and practiced team can significantly improve recovery quality.

When scheduling rebuild activities and recreating the replication and authentication infrastructure, organizations should prioritize subsidiaries and locations that have the highest user populations, perform the most essential services and otherwise have the greatest business impact.

Systems should be allowed online again only if they are hardened (following the known good configuration) and included in the monitoring and endpoint detection and response tooling.

Other typical challenges and questions include:

- How much memory is required?
- Should the same IP addresses be used for rebuilt systems?
- What additional systems are required?
- Which services and teams need to be recovered first to begin reactivating the infrastructure?
- What information goes into and out of the various teams? What are the dependencies?
- What are the dependencies among systems, services and networks? (Search for and fix circular dependencies such as “Active Directory requires database, and database requires Active Directory.”)
- Are gold-standard images available? Determine what “good” looks like (antivirus pattern version, endpoint detection and response tooling, indicators of compromise addressed, patch level, etc.), so that new or cleaned systems are protected.
- Is network bandwidth capable of sending large images? If not, how should images be distributed? Will image recipients know what to do with them?
- Is the available storage sufficient?

If an organization decides to pay a ransom in spite of the known risks and recommendations to the contrary, an experienced third party should be engaged to lead the negotiations. The organization must also define how they will verify the functionality of the key material received from the threat actor and how the decryption process should take place. Bear in mind that it can take more than 24 hours to decrypt a single system.

4.1. Typical ransomware response timeline

Every incident response differs, even if the various remediation activities are similar. The complexity of the response effort and the time required to repair the situation depend on many factors such as organization size, structure, type of malware, scope of the breach, network topology, industry type and cyber-maturity.

In DXC's experience, it may take 1 to 3 weeks to regain production services after a major, large-scale attack, with a month to a year afterward spent on further recovery and security improvement initiatives. During all phases, teams should assume the breach is still active.

Large organizations faced with significant remediation will have to find creative ways to streamline or speed up various tasks.

For example, if the organization has 100,000 impacted clients to rebuild and deploy, and it takes a week to repair 3,000 clients, a full rebuild could take 34 weeks — a timeline that would probably be unacceptable to senior management and could threaten business health or even survival.

An example of a ransomware timeline for incident response and recovery is shown in **Figure 5**.

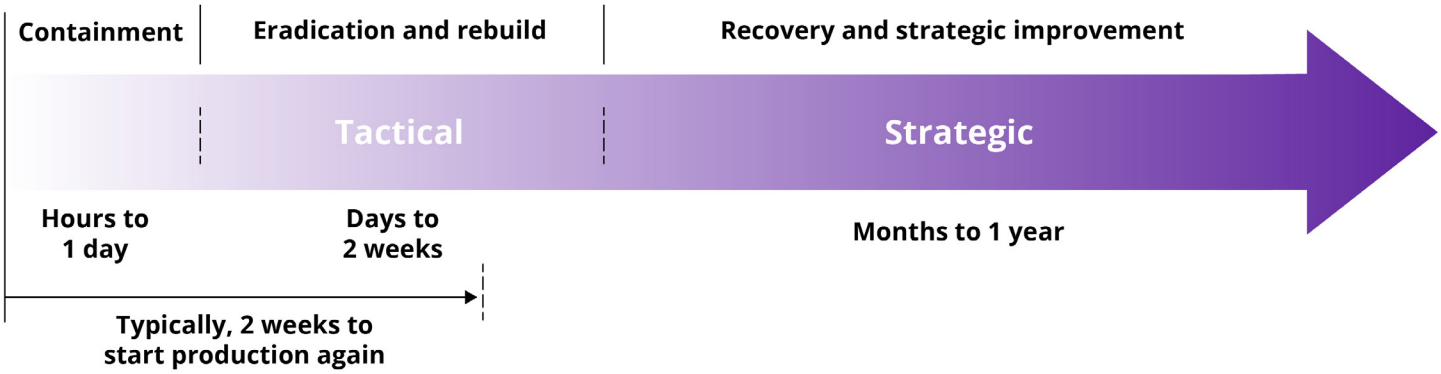


Figure 5. Example of ransomware response and recovery timeline

5. Post-incident activities and lessons learned

DXC highly recommends initiating further strategic security improvement projects once services have been recovered and systems are up and running again. (In the words of Winston Churchill, “Never let a good crisis go to waste.”)

It’s best to seek approval for these strategic projects immediately following a crisis, while senior leaders’ attention is still focused on the impact of the attack.

Post-incident activities should include the following:

- Conduct a cyber-maturity review of the entire security environment to identify gaps and prioritize projects.
- Analyze and update security governance practices.
- Improve operational security reporting capabilities.
- Perform adversary disruption exercises.
- Improve containment and remediation planning and execution.

Consider conducting a business impact analysis and related assessments to get an overview of your organization’s needs, and then prioritize the projects that will yield the best overall improvement.

Conclusion: keys to survival

By following the recommendations in this ransomware survival guide, organizations can mitigate the impact of a ransomware attack on the business, speed up recovery and reduce the chance of another compromise. However, experience shows that investing in prevention and protection before an incident occurs is significantly easier and less expensive than conducting recovery and clean-up under attack conditions. Even better, organizations can avoid potential business interruption and reputational damages. In today's threat environment, proper planning, preparation and governance are the keys to survival.

10 ransomware survival principles: Which can you address today?

Keep these survival principles in mind: Which ones can you address today to improve your cyber resilience?

1. Responding to a ransomware attack without preparation is more expensive and less effective than making proactive improvements and having a planned response.
2. Outdated operating systems and unpatched software-basics of cyber hygiene are generally involved in the initial breach.
3. A backup that is not isolated and protected is only marginally better than no backup at all.
4. Rebuilding without improving the environment leaves organizations no better than they were before the attack, and subject to recompromise.
5. Paying the ransom does not sufficiently protect the organization from recompromise and information disclosure, nor does it ensure that all data can be recovered.
6. Companies should always assume that identity compromise, credential theft and/or privilege elevation of privileged accounts has occurred during a ransomware attack.
7. Using cloud technology does not in itself protect the organization from ransomware attacks.
8. Insufficient network segmentation leaves more endpoints vulnerable to compromise in the event of an attack.
9. Nonexistent or weak visibility into the organization's infrastructure and configuration magnifies the impact of ransomware and slows the response.
10. Threat actors are not just focusing on Microsoft products but will exploit weaknesses in any systems to which they can gain access.

About the author

Lars Klinghammer is a strategist, cyber security architect and global remediation lead in the Security practice at DXC Technology. With more than 25 years of experience in security consulting, he helps businesses proactively improve security, respond to attacks and recover the IT environment. Previously, he was a global cyber security architect in the Microsoft Cyber Security Global Practice where he helped customers improve identity and access management, secure environments and implement security improvement plans.

DXC in security

Recognized as a leader in security services, DXC Technology helps customers prevent potential attack pathways, reduce cyber risk, and improve threat detection and incident response. Our expert advisory services and 24x7 managed security services are backed by 3,000+ experts and a global network of security operations centers. DXC provides solutions tailored to our customers' diverse security needs, with areas of specialization in Cyber Defense, Digital Identity, Secured Infrastructure and Risk Management. Learn how DXC can help protect your enterprise in the midst of large-scale digital change.

Learn more at **dxc.com/security**

About DXC Technology

DXC Technology (NYSE: DXC) helps global companies run their mission critical systems and operations while modernizing IT, optimizing data architectures, and ensuring security and scalability across public, private and hybrid clouds. The world's largest companies and public sector organizations trust DXC to deploy services across the Enterprise Technology Stack to drive new levels of performance, competitiveness, and customer experience. Learn more about how we deliver excellence for our customers and colleagues at **DXC.com**.