DXC TECHNOLOGY

Ransomware defense guide: Prepare for an attack

Follow this checklist to secure systems and data against ransom-based malware

435%

Increase in ransomware attacks since 2020.[1]

$60M

Amount of some of the largest-known ransomware demands.[2]

Confronting the ransomware threat

Ransomware has emerged as one of the most widely used and disruptive forms of cyber attack. Since 2020, ransomware attacks have increased by an estimated 435 percent, and malware is now widely available on the dark web in the form of ransomware-as-a-service applications.[1] In recent years, ransom demands have skyrocketed from hundreds of thousands of dollars to upwards of $60 million.[2] Recent attacks have resulted in devastating consequences for many organizations, with far-reaching societal impacts such as fuel shortages, supply chain disruptions and the interruption of government services.

The constant barrage of successful attacks has shown that most organizations are vulnerable and unprepared for ransomware.

As one of the world's leading security services providers, DXC Technology works with global companies and public sector agencies to harden their systems and protect their data against the latest tactics, techniques and procedures used by sophisticated threat actors. DXC draws on decades of experience in risk management, cyber defense design, deployment and program management, forensic analysis, and remediation to help organizations thwart ransomware attacks.

This ransomware defense guide provides security organizations with a checklist to identify weaknesses in their environments that could be exploited by ransomware, so they can reduce their attack surfaces and lower the likelihood of successful attacks. It also is designed to help organizations conduct self-assessments to determine their security risks and the efforts needed to reduce those risks. In Ransomware survival guide: Recover from an attack, we provide tips on regaining control of your IT environment and minimizing the business impact.

This guide examines key areas of consideration:

- Configuration weaknesses
- Estimated time, cost, priority and impact of ransomware threat mitigation
- Description of typical vulnerabilities
- Recommendation for action

Failure to address items in this checklist may pose significant risk and leave organizations vulnerable to ransomware and other cyber threats.

1 "2020 Cyber Threat Landscape Report," Deep Instinct, February 2021.
2 "Cybersecurity in the Era of Intelligence and an Expanding Attack Surface, Harvard Business Review Analytics Services, July 2021.

Typical configuration weaknesses

Configuration weaknesses are some of the most common vulnerabilities that enable successful ransomware attacks. These weaknesses fall into three main risk categories: business, technical and operational.

1 Business risks

Organizations must create a culture that encourages employees to rethink and challenge current operational practices.

Often, technical activities, risk management strategies and security procedures are poorly aligned with the business. Most organizations tend to prioritize business needs first. It's not unusual for companies to decide against shutting down or isolating systems verified as compromised in order to make sure they can still support related business functions. This is not recommended, as it creates opportunities for threat actors to further compromise the environment.

The business demand for availability of services typically conflicts with the confidentiality and integrity required during an investigation, including the need to preserve evidence, which can help determine whether data has been exfiltrated. The business is often focused on restoration, and this, together with the nature of ransomware encryption or some of the techniques deployed by ransomware threat actors, denies or frustrates evidence gathering.

1.1 General mindset and cultural aspects

Weak approach

Often when new solutions or technologies are to be implemented, management perceives IT security as an obstacle and cost driver with poorly defined return on investment. Administrative teams frequently violate basic security principles for ease of access and convenience. They often don't realize that this carelessness could put the entire organization at risk by introducing new attack vectors. A typical mindset is, "We've always done it this way."

Recommended approach

Time: Medium to long term

Cost: Low

Priority: 3

Impact: High

Organizations must create a culture that encourages employees to rethink and challenge current operational practices. Businesses should assume they have been compromised and align operational processes accordingly. It is important to educate teams that change is something that can help to broaden experience and includes new opportunities to solve required tasks more efficiently and securely.

1.2 Know your crown jewels: Determine which assets are essential for the organization's survival

Weak approach

Business and IT teams often have different understandings of what is essential to the organization. A typical IT team's comment in maturity assessments is: "Management doesn't understand what is required." IT teams, therefore, have a tendency to make their own decisions about priorities. Often during normal day-to-day operations they do not bother to define which business services are essential, and only scramble to prioritize them when an incident happens, when the organization is under pressure and in a crisis. This lack of distinction often results in equal security controls for all entities in the environment, insufficient security controls for high-value target systems or excessive security controls for low-value target systems.

Recommended approach

Time: Short to medium term

Cost: Low

Priority: 1

Impact: High

Organizations should know which IT systems are required to build and support essential business services. Based on that knowledge, organizations can plan how to safeguard essential solutions appropriately with the right level of protection across all layers of an in-depth model of defense. It is also imperative to understand all possible dependencies for other services or systems that may be required to operate these services. In recent attacks, for instance, DXC has observed threat actors purposefully targeting backup solutions to further frustrate or impede the organization's recovery efforts.

1.3 Know how to assign security layers: Assign each single system to only one security layer

Weak approach

It is challenging for an organization to define what assets are crucial systems and which systems are less critical. To make such a determination under attack conditions is more difficult than developing a proactive, well-defined and documented discussion and decision process. Lack of planning can lead to confusion and less effective incident response.

Recommended approach

Time: Medium term

Cost: Low

Priority: 1

Impact: High

Review the organization's configuration management database (CMDB) and plan a decision process that defines the security tiers, with tier 0 being the most secure and tier 2, the least. In other words, know the landscape and terrain you are defending. Ideally, documentation should define how long the organization can survive without the affected services and related IT infrastructure.

1.4 Legal support

Weak approach

Enforcement authorities in many jurisdictions are considering penalties for paying ransoms, viewing it as complicit with criminality, and there are no guarantees that payment gets you full access to your data.

When a successful attack occurs, victims of ransomware are immediately under pressure to decide whether to pay the ransom. Organizations are advised not to pay, as such payments only encourage the criminal business model. In fact, enforcement authorities in many jurisdictions are considering penalties for paying ransoms, viewing it as complicit with criminality, and there are no guarantees that payment gets you full access to your data. Still, many organizations — especially ones with low security and operational maturity and little to no option of recovery — do consider paying. Organizations typically want to handle these situations on their own without third-party support. However, recent studies have shown that organizations that pay ransoms still incur recovery costs — and that they ultimately almost double their restoration costs by paying the ransom.

Recommended approach

Time: Short term

Cost: Low

Priority: 1

Impact: Medium

The standard industry recommendation is to not to pay the ransom, but if organizations decide to pay, they should consider involving legal experts and third-party crisis communication professionals who have experience negotiating with criminals and communicating with the media, employees, shareholders, partners and other stakeholders.

A key element of negotiation, for instance, is to ensure that the threat actors can demonstrate the ability to decrypt the affected data. In addition, the attackers may have stolen sensitive data to further pressure victims by threatening to release that data publicly.

This is why it's important to retain these experts before an attack occurs. Third-party professionals will already have an understanding of the organization's needs and priorities and can quickly help resolve important questions during a crisis:

- How is the decryption key derived?
- What does a sufficient verification of function look like?
- How is the key distributed to the various systems?
- How do you prioritize system decryption?
- How do you make sure the systems are cleaned before they are decrypted and that they don't get immediately re-encrypted?
- How large are the file servers, databases and other large systems, and how long does it take to decrypt those systems?
- Which is faster, decryption or restore, and how much data loss is associated with each?
- How much storage is available? (It is very likely the organization will want to copy the encrypted data to a safe location in case something initially goes wrong while testing the decryption process.)
- What's the best way to communicate the attack, the impact on the business and the reason for paying or not paying the ransom to internal and external audiences?

1.5 Supporting strategic initiatives: Prepare for the future

Weak approach

Security strategies are often not aligned — or not sufficiently aligned — between the business needs and technical implementations of solutions. In a ransomware crisis, it could take time for all relevant parties to agree on prioritization, potentially wasting precious time on less important systems. Developing a business continuity plan (BCP) can help clarify priorities in advance.

Recommended approach

Time: Medium term

Cost: Low

Priority: 2

Impact: Medium

Since improving and preparing an IT organization takes time, we recommend activities and planning that will improve the resiliency and efficiency of managing potential ransomware attacks. The key is to further institutionalize the chief information security officer (CISO) role into the org chart and drive the board of

directors' understanding of the risks and potential impact of an attack, as well as the need to invest in preparation.

The most important countermeasure to ransomware is a sufficient backup strategy and practice — planned, tested and regularly updated and documented.

2 Technical risk

Challenges associated with preventing successful ransomware attacks at the technical level are significantly broader than those at the business level. The following list is not exhaustive but covers the most frequently observed weaknesses in technical environments.

2.1 Backup

Weak approach

Backup capabilities are an old but still pertinent topic. Backups are critical assets and should be cherished and adequately protected. Common issues are:

- No backup at all for essential systems
- No or only partial backup from subordinated Active Directory domains and domain controllers
- Unstable backups; no exercise backup strategy or plan
- Backups that are on systems or online and are also victim to the ransomware
- No know-how or training to quickly rebuild from the backup
- Dependencies between backup systems and encrypted systems

Recommended approach

Time: Medium term

Cost: Low

Priority: 1

Impact: High

The most important countermeasure to ransomware is a comprehensive backup and restore strategy — planned, tested and regularly updated and documented. Relevant parts of the organization must be trained regularly in backup and recovery. Securely store additional backups offline or in an air-gapped vault to protect them from ransomware threat actors who will look to damage them to prevent recovery.

2.2 Vulnerability management

Weak approach

Vulnerability management, an important part of endpoint and network security, is the practice of routinely identifying, prioritizing and mitigating software vulnerabilities. DXC often sees organizations neglect vulnerability management

and fail to follow recommended practices. Patch management is a significant issue in many organizations, but organizations also fail to sufficiently address system updates, mapping of assets and regular vulnerability scanning.

Recommended approach

Time: Medium term

Cost: Medium

Priority: 2

Impact: High

To proactively improve security and prioritize threats like identity and credential theft, DXC recommends allocating additional budget to vulnerability management. This typically includes spear-phishing simulation, penetration testing, adversary emulation and red team/blue team exercises **(Figure 1)**.

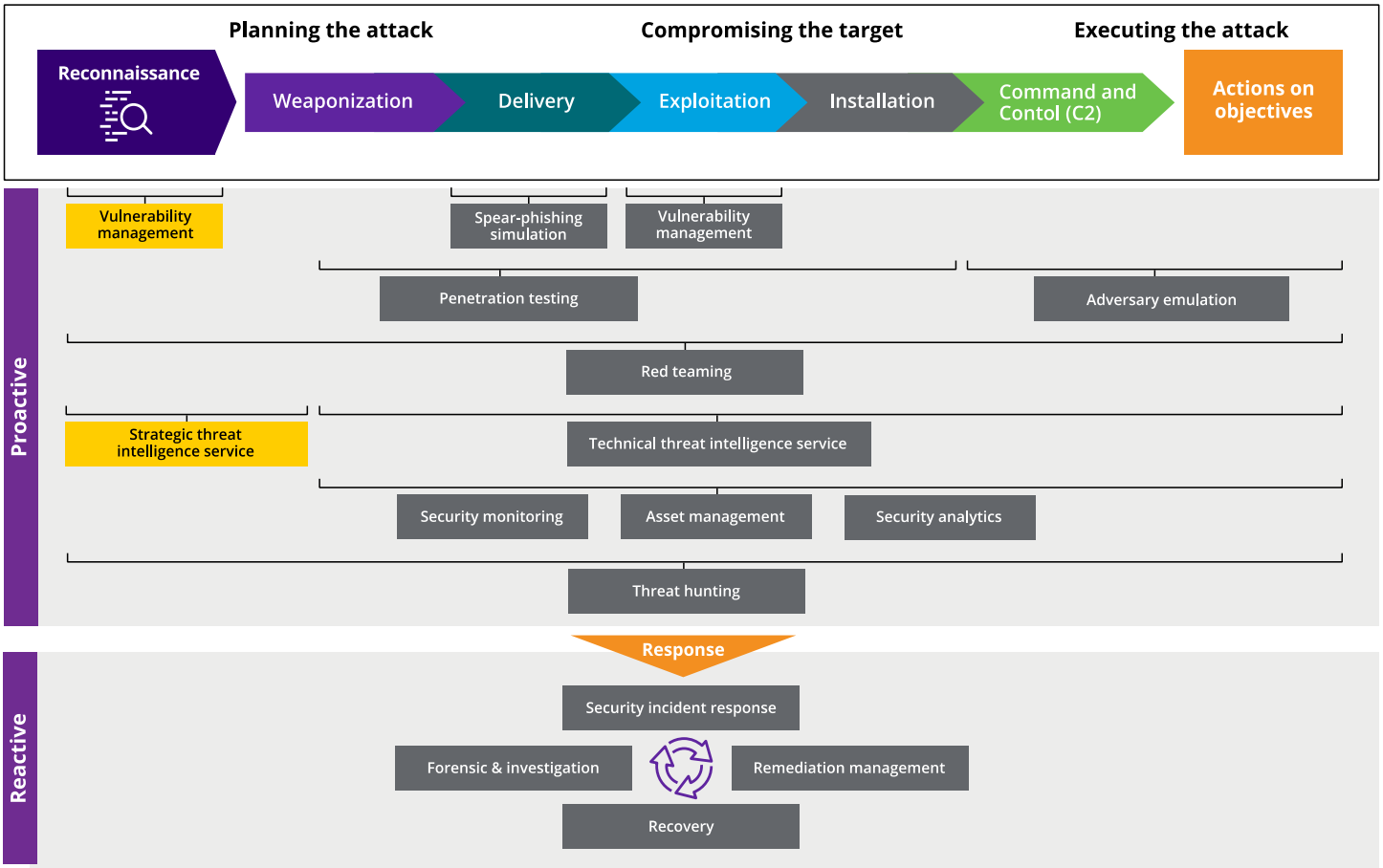

Figure 1. Security disciplines and related domains

2.3 Patching server and client apps

Weak approach

Updating, including patching, is an important countermeasure in a protection strategy. We typically see a variety of shortcomings, especially related to shadow IT:

- No patching at all
- Old patch status
- No patching strategy
- No compliance testing
- Beta software
- No firmware updates for assets (routers, firewalls, printers, etc.)
- No BIOS updates
- Outdated operating systems
- Old apps, systems and special solutions that are not patchable because they are losing support or are insufficiently isolated
- No control mitigation for required legacy systems
- Expected outdated patch status related to use cases. For example, in the military, submarines may under the polar ice for more than 6 months and have no access to patches.
- No consistent and defined standard, not only for OS patches but also for MS Office, PDF readers and other typical applications found in enterprise environments

Recommended approach

Time: Medium to long term

Cost: Low

Priority: 1

Impact: High

Updates, including patches, can prevent a broad spectrum of threats. We recommend planning for these activities and regularly reevaluating the planning and implementation.

2.4 Network visibility

Weak approach

Good network visibility is as important as endpoint visibility. Manufacturing and related industries typically face a common challenge of deploying endpoint detection and response (EDR) agents on operational technology systems, and often the only option is to ensure good network visibility for the endpoints in scope.

Recommended approach

Time: Medium to long term

Cost: Medium

Priority: 2

Impact: Medium

Strong endpoint and network visibility is important, and it can help detect suspicious activities on systems that can't be protected through EDR tooling.

Strong endpoint and network visibility is important, and it can help detect suspicious activities on systems that can't be protected through EDR tooling. DXC regularly sees threat actors benefit from situations in which security teams have insufficient network visibility. Strong endpoint and network visibility is important, and it can help detect suspicious activities on systems that can't be protected through EDR tooling. It also helps when threat actors realize they have been detected and then change their tactics, tools and procedures to hide their persistence. Organizations should try to follow a layered approach in which deeper control can stop suspicious or malicious activity missed at a higher level.

2.5 Identity life cycle

Weak approach

Many severe security incidents involve an identity and credential component. Typical issues include:

- A large number of active highly privileged accounts (administrator, domain admin, enterprise admin, schema admin, account operator, etc.)
- A large number of disabled or unused privileged accounts — even if disabled, accounts can be used to hide persistence
- Many privileged accounts that haven't logged in even after 100+ days — why maintain accounts that are not used?
- Many privileged accounts with a service principal name (SPN) assigned
- Passwords that are shared by several individuals and haven't been changed in 100+ days
    - This is a hot topic, especially for service accounts, where it is often the case that passwords are not changed regularly and high privileges are not required. This is a complex topic in "old, grown" environments.

Maintain a rigorous credential hygiene regimen. Eliminate old, unused privileged accounts and reduce the overall number of privileged accounts.

- Account passwords older than 365 days for KRBTGT, an account used for Kerberos, the default Microsoft Windows authentication protocol
    - If compromised, this weakness enables Kerberos "golden ticket" attacks, giving attackers access to any resource on an Active Directory Domain. Microsoft has released a support script and documentation for preventing these attacks.
- Unchanged admin count value still on 1, as this blocks the application of changes to those accounts
- Excessive use of group nesting so that admins have no overview of the real, cumulated permissions
- No monitoring of privileged groups and accounts
- Insufficient life-cycle management
- No privileged account management (PAM) software or other protection solutions
- No multifactor authentication
- No separation of duties
- No security tiers

Recommended approach

Time: Medium to long term

Cost: Low to medium

Priority: 1

Impact: High

Maintain a rigorous credential hygiene regimen. Eliminate old, unused privileged accounts and reduce the overall number of privileged accounts. Usually, privileged groups should be empty and should be protected using PAM solutions or similar controls. Apply separation-of-duties practices for each type of account.

2.6 Multifactor authentication

Weak approach

Privileged accounts without strong authentication make it significantly easier for threat actors to compromise systems. Environments that fail to make multifactor authentication mandatory at least for privileged accounts are at even greater risk. Organizations should be aware that by default, devices such as smart cards just mask the password task. Technically, for attacker tools such as Windows Credentials Editor or Mimikatz, there is no significant difference between a password from a human and a password hash used during Standard Chartered (SC) login. The SC login should also be protected.

Organizations should proactively address standards and compliance in advance to provide a good understanding of how systems are expected to be set up and configured.

Recommended approach

Time: Short to medium term

Cost: Medium

Priority: 1

Impact: High

The industry recommendation is to use multifactor technology to protect highly privileged credentials. DXC further recommends regularly changing passwords for those accounts and not sharing privileged accounts between individuals and systems, including help desk and operations teams. Identity and access management tools are available to support these controls. In addition, we recommend PAM solutions.

2.7 Technical and configuration standards and compliance

Weak approach

A typical scenario involves outdated or incomplete security standards, often coexisting with inadequate verification approaches, that can lead to inconsistent configurations across equal types of systems. These issues make it hard to estimate the risk for the various solutions and systems and to detect unexpected behavior and potential vulnerabilities.

Recommended approach

Time: Medium term

Cost: Low

Priority: 2

Impact: Medium

Rather than focusing on compliance during an ongoing attack, organizations should proactively address standards and compliance in advance to provide a good understanding of how systems are expected to be set up and configured. In addition, organizations should implement all hardening activities following a defense-in-depth approach that includes system-specific controls (e.g., local passwords). A description of a holistic approach to cyber security and defense is defined in the DXC's Cyber reference architecture, shown in **Figure 2**.

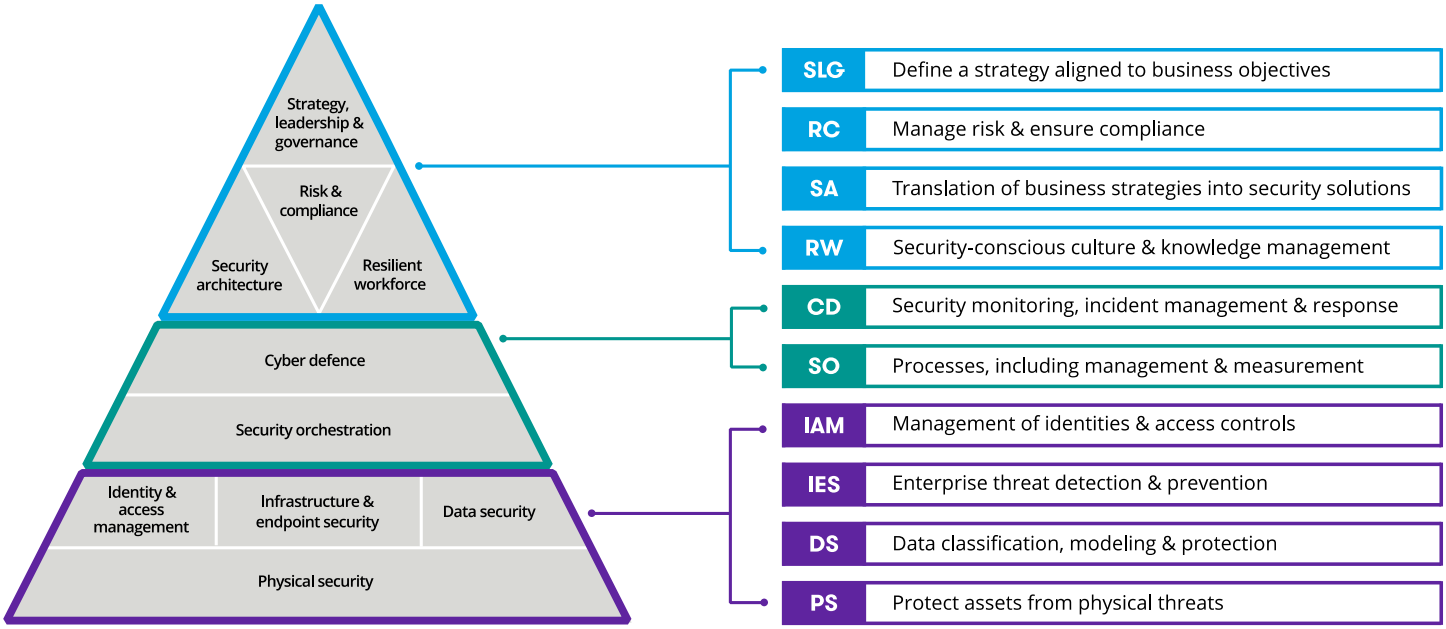

Figure 2. Domains of the DXC's cyber reference architecture

2.8 Network segmentation and remote access

Weak approach

Network design has a significant impact on the ability of ransomware to spread within an IT infrastructure. DXC often finds that customers have flat networks with very little segmentation. These conditions can enable ransomware to have a larger impact.

Recommended approach

Time: Long term

Cost: High

Priority: 2

Impact: High

The effort to plan and align network design with security boundaries is significant, especially for environments that are large or have grown over time. Nevertheless, an organization should think about introducing segmentation for the most essential systems and services. This includes Tier 0 entities and firewall and border systems such as servers on a separate security zone and VPN systems.

We also recommend adhering to an isolation approach, making sure that there is as little connectivity as possible between different security layers. In its most extreme implementation, this approach makes all systems redundant and isolated from each other.

The degree of implementation depends on an organization's risk appetite, but all companies should ensure that only specific address pools or systems are technically capable of connecting to secured systems. Newer approaches — microsegmentation combined with virtualization technology — bring segmentation even deeper into the data center infrastructure.

2.9 Antivirus

Weak approach

It is generally recognized that antivirus software is less effective, and some IT professionals hold the view that in today's threat landscape, antivirus software is not up to the task of protecting systems. However, it still has a role to play in providing some security controls. For the most part, antivirus solutions are widely available in most organizations, far more so than EDR.

Recommended approach

Time: Medium to long term

Cost: High

Priority: 2

Impact: High

When organizations are faced with a breach, they should always consider deploying EDR tooling to assist with the investigation, gain visibility of the environment and add further security controls. They can still leverage antivirus technology, since identifying components used by malware is often challenging, and it is important to be able to identify malware samples quickly.

Where possible, identify network-based indicators but also provide samples to antivirus vendors so a signature set can be produced for deployment across the environment to aid identification and recovery. DXC recommends focusing on future strategies toward machine learning and anomaly detection capabilities. These newer technologies are faster and have more capabilities that will help organizations detect ransomware and related suspicious activities in their IT environments.

3 Operational risks

In addition to the technical controls previously mentioned, a key area of defense encompasses operational approaches, processes and procedures that are used to maintain and run IT environments. The following approaches represent the most important practices for proactively addressing operational risks and reducing the attack surface for ransomware and related threats.

Organizations need a defined security monitoring approach that articulates standard as well as suspicious or malicious use cases.

3.1 Security monitoring

Weak approach

Threat actors often gain access to an environment weeks or months before they are discovered, and this lead time enables them to hide and dig in. Effective security monitoring can help organizations detect suspicious activity quickly. DXC frequently observes significant weaknesses in this area. Ensuring monitoring and visibility of endpoints, the network and the authentication layer is essential for any organization.

Recommended approach

Time: Medium to long term

Cost: Medium to high

Priority: 1

Impact: High

Organizations need a defined security monitoring approach that articulates standard as well as suspicious or malicious use cases. Security teams must build and maintain appropriate filters and corresponding rulesets for automated countermeasures. The goal is to detect threat actors as early as possible. Many commercial tools and services are available from a variety of vendors. It is important to recognize that many solutions utilize static use cases that often become stale, so these tools need to be maintained and refreshed.

3.2 CMDB and asset management: You can protect only what you know about

Weak approach

During discussions with customers who suspect that their organizations have been breached, DXC often finds that organizations do not have complete views of their IT environments. Their information may be incomplete or out of date. Sometimes complete solutions are not mentioned. Patch levels, OS versions and more may not be documented. System owners may be missing or not updated. If firewall, network and other systems are outsourced to a third party — or to several third parties — an organization faces common challenges such as lack of accountability and outdated or expired support contracts.

Another related issue is shadow IT. If security policies allow users to stand up their own infrastructure without integrating it into tooling and support, an organization can quickly end up with an unprotectable environment. It's not unusual for a system to become orphaned, without an owner, often forgotten and therefore unmanaged, adding an attack vector and an easy-to-exploit system.

Recommended approach

Time: Long term

Cost: Medium to high

Priority: 1

Impact: High

Asset management is difficult and time consuming, but if organizations don't know what they have, they can't protect their environments. In addition, rogue systems often run essential services that can't be migrated on short notice. We recommend beginning the search for unmanaged systems and then decommissioning, updating or isolating them as required. These kinds of systems act as locations for attackers to get into the environment or hide their persistence.

3.3 Incident response processes — runbook creation

Weak approach

Organizations need to be proactive in designing comprehensive emergency and incident response plans. For example, in one situation, a company needed to restore power but realized too late that the pumps that delivered fuel to the emergency generators ran on electricity. In another situation, the organization needed a database to rebuild the Active Directory, but realized they first needed an Active Directory to rebuild the database. When it comes to ransomware, many organizations do not have detailed plans for what to do if large parts of their IT organizations and dependent areas are affected. Imagine: telephony, access control, SCADA systems and production machines not working, or not working sufficiently, all at the same time. Typically, with the exception of applications that affect health and protect lives, organizations don't know which of their systems are top priority.

Recommended approach

Time: Medium term

Cost: Low

Priority: 1

Impact: High

Plan incident response by using simulated situations in which a large number of systems are unusable or destroyed, including the data processed by these systems. Examples of dependencies to plan for: who requires new machines immediately, which teams are essential, how to restart the business, what alternative processes and manual approaches look like, which groups of systems are required and which are not, what mandatory prerequisites there are, what can be temporarily ignored, what legal requirements there are, and more.

All of these topics can fill a 30-page document. They are closely dependent on business impact analysis and business continuity planning and should be aligned with them.

3.4 Roles and responsibilities

Weak approach

During an emergency such as a ransomware attack, it is important to prioritize, structure and plan quickly. A good understanding of roles and responsibilities is an integral precondition for such preparation, but this understanding is often missing or not sufficiently communicated across the organization. Typically the following groups are involved: executive management, legal, service providers, forensics, governmental organizations, operations, employees, help desk, human resources, incident handling, customers and the public. Without defined roles and responsibilities, orchestration of these groups can be challenging.

Recommended approach

Time: Short to medium term

Cost: Low

Priority: 1

Impact: High

This area of security planning requires proactive planning and regular review, finetuning and updates. Organizations should plan for a situation in which nothing is working — no email, no telephone systems and no access authorization or other IT infrastructure-dependent enterprise services. Proactively communicate finished plans. Prepare a war room. Plan and regularly assess out-of-band communication. Use many different playbooks for many different scenarios. During ransomware attacks, it is crucial to designate strong leaders who can make difficult decisions with minimal information and can delegate tasks to other strong leaders who can structure and drive the recovery exercise.

3.5 Cyber maturity assessment

Weak approach

Management teams and delivery units often hold wide-ranging perceptions of their organization's level of cyber maturity. While management assumes a high maturity level and structured plans, the operations team often knows nothing about either. DXC recommends regular security maturity assessments so that any shortcomings can be addressed proactively.

Get the latest threat updates

Protect your enterprise. Subscribe to DXC's monthly report on the latest threats, breaches, cybercrimes and nation-state activities.

dxc.com/threats

Recommended approach

Time: Short term

Cost: Low

Priority: 1

Impact: High

Perform a comprehensive assessment to get an accurate status of an organization's security maturity, ideally compared with its competitors and the industry as a whole. Use the findings to develop a prioritized improvement roadmap, keeping in mind that attempting to "boil the ocean" can strain resources and reduce the overall impact of the assessment. Consider fewer but accurate, prioritized activities.

Conclusion: Taking the next steps

Organizations have many factors to consider in ransomware defense planning. Following these recommendations will help in preparing for and mitigating the effects of ransomware incidents. Not all attacks can be prevented completely, but with the right planning, organizations can significantly reduce the effects of a ransomware attack and recover quickly.

About the author

Lars Klinghammer is 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.

Visit
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**.