Trellix

The CISO's Guide to Ransomware

How to prepare your organization
to take action when every minute counts

TABLE OF CONTENTS

THE CISO'S JOB JUST KEEPS GETTING HARDER

As a CISO, you're responsible for protecting your organization. That core mission isn't static, it's changing every day. You're facing evolving geopolitical factors, an expanding attack surface, complex architectures and toolsets, cost constraints, SOC analysts who are burning out, and a board who may not understand what you're up against.

In a global survey of CISOs for "Mind of the CISO: Behind the Breach," 37% reported they had managed a ransomware incident. The same research makes it clear that cyber incidents are increasingly complex and sophisticated. CISOs report an average of three causes per incident, indicating that attackers are employing multiple avenues and tactics to breach defenses. In a troubling sign, the number one cause they cited was technology failing to detect an attack (42%).

Technology is failing to keep up, even as the speed of attacks is accelerating. The median dwell time for a ransomware attack used to be nine days. A recent industry report now puts it at 24 hours or less.

When it comes to ransomware, every minute counts. This eBook aims to empower CISOs and cybersecurity leaders at organizations of all sizes with road-tested guidance on combating ransomware.

"Experiencing a cyber incident reinforced the concept that we need to be ever-vigilant, and no matter how secure we think we've gotten things, no matter how many tools we have in place, it's a constant battle."

– CISO of a U.S.-based manufacturing company

DEBUNKING COMMON RANSOMWARE MYTHS

Ransomware detection and response is complex and requires orchestration. As a CISO, you're the critical connection point between different teams and functions. You can help your organization get set up for success by debunking common misconceptions about ransomware.

Myth 1: There's a ransomware silver bullet

Technologists may focus on a silver bullet for ransomware. Imagine if you could buy a technology that just makes it go away. Unfortunately, such a silver bullet doesn't exist. Ransomware is not simply a technology challenge. It's also a process and architecture challenge that you solve operationally.

Myth 2: Becoming ransomware resilient means you need to redo everything

After an incident, you may be tempted to change all your technology and swap everything out. But a successful ransomware incident typically has multiple causes. What matters most is having layered visibility and controls at as many vectors as possible.

Myth 3: Ransomware is a single event that follows a specific playbook

There are different phases to an attack, and there are multiple causes for an incident. Different ransomware gangs employ different techniques. Some attacks happen very quickly to avoid detection. Others may take several days and leave ransomware behind so that defenders are hit a second time after they believe they've solved the problem.

Myth 4: Ransomware strikes only large organizations

News headlines are full of reports about large multinational organizations suffering from ransomware attacks. However, our research shows that attackers target organizations of all sizes. Smaller organizations may in fact be more vulnerable because they typically lack the security resources of large multinationals.

Myth 5: Ransomware is a security problem

Ransomware is an organizational problem that needs attention at the highest levels. Our Mind of the CISO: Behind the Breach report indicates that for many organizations, board-level support for cybersecurity increases after an attack, but is lacking before an attack occurs. Educating the board becomes one of the CISO's most important challenges, a topic we'll cover in the next section.

> **"The biggest learning is the awareness had to be raised at the board level... unfortunately, it had to take an incident to do so."**
>
> – CISO of an Australian government agency

THE CISO AS CHIEF COMMUNICATOR

“A CISO serves as chief communicator and chief educator around risks like ransomware. It’s up to us as leaders to be effective communicators and explain these issues.”

– Harold Rivas, CISO, Trellix

CISOs who engage with business stakeholders will have greater success in protecting their organizations from ransomware.

However, it can be challenging to communicate about ransomware risks and defensive strategies to leaders who don’t have a cybersecurity background. It’s important to find a way to insert yourself into top-level conversations with your board so you can help them understand the risks facing the organization and get their buy-in for taking appropriate action. Let them know that when you see something that looks like ransomware, you need to take direct action instead of continuing to study it for fear of disrupting the business.

For instance, ask your CFO: If my responsibility is to protect the organization, if I detect something in the middle of the night that looks like a ransomware campaign coming from your account, do I have your support to take the right actions to protect the organization? Most likely, your CFO is going to say yes.

Leverage those relationships at the top of the organization so there’s a willingness to make the kind of tradeoffs that are necessary. It’s critically important to give your SecOps teams, your engineering leaders, and your infrastructure partners the green light with the right support at the top of the organization.

The next section dives into the steps you can take to increase your cyber resiliency and get ransomware ready.

10 BEST PRACTICES FOR CISOs TO GET RANSOMWARE READY

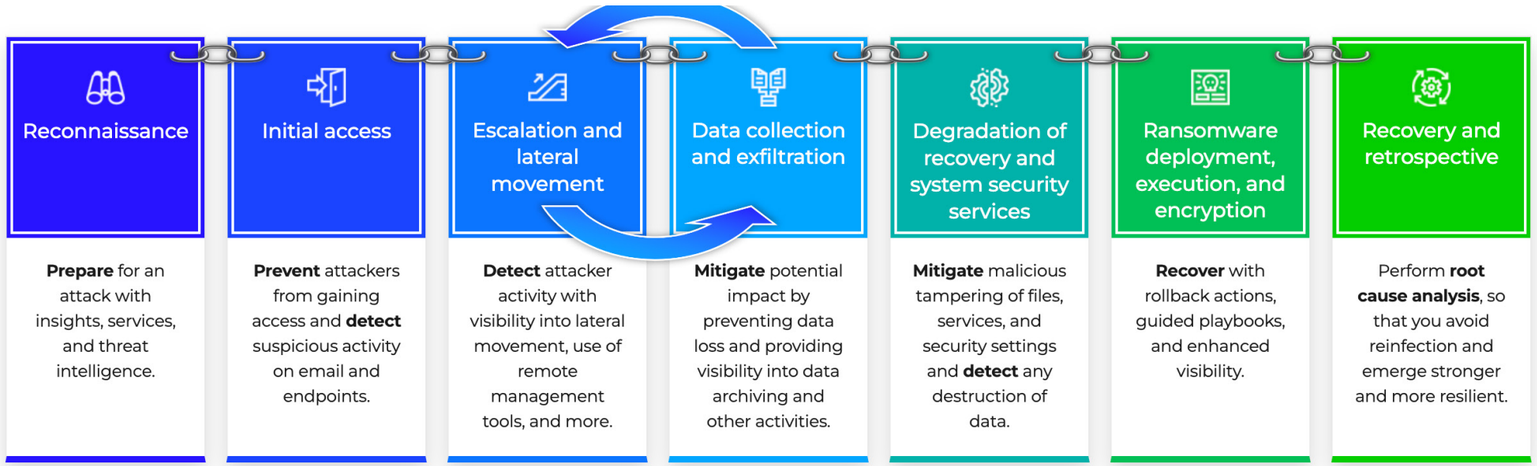
Ransomware threat actors are constantly changing their methods. We've compiled a set of best practices that can help you prepare for this always evolving threat.

"I think of the Navy SEALs when we get ready for ransomware. They are constantly training and working together."

– VP and ISO of a U.S.-based financial services company

1 Understand the anatomy of a ransomware attack

To defeat ransomware it's essential to understand how ransomware enters and moves through your environment. A typical ransomware attack involves multiple phases. At each one, there's an opportunity to shut down the attack. The Trellix Advanced Research Center developed a seven-stage kill chain model after analyzing more than 9,000 real-world attacks. Use the Trellix ransomware kill chain to assess the capabilities you need in your organization and plan for each phase. If you do have an incident, don't forget the Recovery and Retrospective stage to uncover root causes and emerge stronger and more resilient.



Questions to ask:

- How many phases of the kill chain are you currently able to cover?
- What capabilities do you need to cover more?
- Do you have a feedback loop in place to learn from incidents?

10 BEST PRACTICES FOR CISOs TO GET RANSOMWARE READY

2 Create a strong foundation with IT best practices and education

Basic but essential measures such as enforcing strict password policies, are your first line of defense. Network segmentation, multi-factor authentication (MFA), and strong backups are all ways you can increase your resilience.

Some concrete defensive tactics are relatively easy to implement. For instance, you can create dummy or honeypot accounts that are not used for anything other than to catch attackers trying to enumerate your Active Directory store. For extra credit, create an account that starts with an A so it's at the beginning of the alphabet and create one that starts with a Z so it's at the end. Regardless of which direction the attacker is attempting to enumerate your Active Directory tree, you will have an opportunity to catch those early indicators immediately.

Questions to ask:

- Do employees receive regular security training?
- Are you using multi-factor authentication?
- Do you enforce strict password policies?

3 Operationalize threat intelligence

Good threat intelligence can help you make sense of the threat actor landscape. It helps you understand how threat actors are operating, what techniques they're using, and how that is changing over time. Threat intelligence enables you to see which ransomware campaigns are most prevalent for your geo and industry and how you can better defend against them. You might depend on multiple sources for threat intelligence, including Trellix, and use AI and machine learning to help you operationalize it.

Operationalizing threat intelligence means doing more than just collecting information. For greatest value, you want to layer it with visibility across your entire IT estate and correlate it with indicators from various telemetry sources. An AI-powered XDR platform like Trellix's makes it possible to move from crisis mode, where you're constantly reacting to alerts, to proactive risk reduction.

Questions to ask:

- Are you using threat intelligence to inform your defense?
- Are you correlating threat intelligence with other indicators?
- Are you using AI and XDR to connect the dots from seemingly disparate events?

10 BEST PRACTICES FOR CISOs TO GET RANSOMWARE READY

4 Assess and manage your risk

As organizations evolve in maturity, CISOs shift their focus from a reactive, threat-based focus to a risk-based approach. For each of the systems that you have, what is the potential for a system compromise, loss of data, or loss of the availability of the system?

As a CISO you should evaluate where the greatest risks to the organization are found and how you can put in place stronger processes and methods for protecting weaker areas. Limited budgets, resources, and time require tradeoffs according to what makes sense for the organization.

Questions to ask:

- Do you know the areas of greatest risk to your organization?
- For areas of greater risk, what would be the impact of an incident?
- Are you actively working on ways to reduce risk and measure risk reduction?

5 Identify your critical data assets

In the past, ransomware may have been focused on disruption and causing a lockout of sensitive files that are critical to your organization. Today, any sensitive information could be targeted in a ransomware campaign. Many ransomware threat actors have started using double extortion tactics: not only do they encrypt the victim's data but also threaten to leak sensitive information unless the ransom is paid.

CISOs should think broadly about information within the organization that needs protection.

Questions to ask:

- Do you know what data is critical to your business function?
- If that data was held hostage would you be forced to pay a ransom?
- Do you employ data security controls including data loss prevention to safeguard your data?

10 BEST PRACTICES FOR CISOs TO GET RANSOMWARE READY

6 Prioritize early detection and be prepared to act

The best outcome is to be able to detect an attack as early as possible. During an early stage of the kill chain, such as Reconnaissance, an attacker may be scanning your environment, gathering information, and phishing for information. Defensive techniques you can use at this stage include setting up dummy accounts to catch attempts to enumerate Active Directory, blocking IP addresses that appear to be scanning your network, and so on.

But CISOs must also balance the need for early detection with the goal of minimizing disruption to the business. Would you bring your business to a standstill if an incident is isolated and contained? Doing the upfront work of communicating risks to your board will pay dividends here.

Questions to ask:

- Have you defined the criticality for various incidents?
- Are you using playbooks to help your team respond?
- Do your teams know when they have the green light to take action even if doing so disrupts the business?

7 Create your information security plan and document policies

Don't forget the governance side of ransomware defense. Preparing your organization involves ensuring you have a robust information security policy and that your executive team and board have reviewed and are aware of the steps you need to take to respond. Consider creating an information security plan that covers various threats, including ransomware. As part of your documentation effort, create specific playbooks for the threats covered under your plan. Start with your information policy, then your plan, and finally playbooks.

Questions to ask:

- What governance documents exist in your organization and do they need to be revisited?
- Have you documented your information security policy?
- Does your documentation include a plan for a ransomware incident?

10 BEST PRACTICES FOR CISOs TO GET RANSOMWARE READY

8 Use XDR to accelerate detection and response

Many organizations have invested in a number of security tools over the years. In a Trellix Mind of the CISO report, CISOs admitted to using 25 tools on average. Yet a complicated tech stack can lead to siloed capabilities and challenges, such as end-to-end visibility, platform management issues, and more. An extended detection and response (XDR) solution can integrate tools and dismantle information silos, providing insights at the speed of AI.

XDR provides much-needed context so that you can detect threats earlier and accelerate your speed of response. Read why XDR is a game changer for CISOs.

Questions to ask:

- Do you have a way to correlate multi-vector detection information?
- Are you looking to consolidate tools and simplify your technology stack?
- Are you able to see how an attack would unfold across your environment?

9 Report on key business outcomes

As CISO, you have metrics to communicate to your CIO and board members. Identify the ones that matter in terms of reporting on the organization's ransomware risk. These will vary according to factors like your organization's industry, location, and more.

Questions to ask:

- How have you reduced mean time to detect?
- Are you reporting incidents in a way that's appropriate for your organization and industry?
- Are you able to report regularly on risks in a way the board understands?

10 BEST PRACTICES FOR CISOs TO GET RANSOMWARE READY

10 Test and assess your capabilities

As you progress your ransomware maturity, make sure to practice your defensive capabilities. Regularly conduct ransomware tabletops and engage in red and blue team exercises. Test your security controls and backup systems. For instance, take your backups offline and restore them. Take a server offline and then see if you can recover that server from scratch.

A professional services engagement can help you conduct exercises that are informed by the latest threats and ransomware TTPs. As the CISO, you are looking to connect teams and stitch together an effective end-to-end response covering email, endpoint, network, data security, and more.

Questions to ask:

- Have you established security baselines?
- Are you regularly assessing your environment?
- Do you conduct red and blue team exercises?

RANSOMWARE AND AI

“Generative AI helps us solve the question of, how do I take a junior SOC analyst and make them 10 times more effective by supporting them and giving them context and color that’s critical to their ability to respond?”

– Harold Rivas, CISO, Trellix

Advances in AI are changing the technology industry and society at large. Many in cybersecurity have sounded the alarm about AI-assisted attacks and how ransomware threat actors are already using AI to evade detection. To take just one example, generative AI can write phishing emails with flawless grammar and spelling.

On the other hand, defenders can expect to use AI to bolster their cybersecurity and make SOC teams more efficient and effective. By harnessing AI, teams can connect the dots on threat intelligence and move from reactive to adaptive security operations.

For cybersecurity leaders, the future of secure operations includes AI in a variety of forms:

- Generating playbooks for a multitude of scenarios
- Prioritizing actions for a SOC analyst to take
- Correlating information from threat intelligence, telemetry sources, and other inputs

EVOLVING YOUR RANSOMWARE MATURITY

By now you should have a better understanding of best practices to protect your organization from ransomware. For true cyber resilience, you should assess where your organization is overall and know what it takes to move up the maturity curve. Here are three stages on the journey to ransomware maturity.

Level 1: Foundational

At Level 1, organizations are building basic capabilities. They likely have endpoint protection, but they may lack additional security controls. They are reactive and may have a few playbooks.

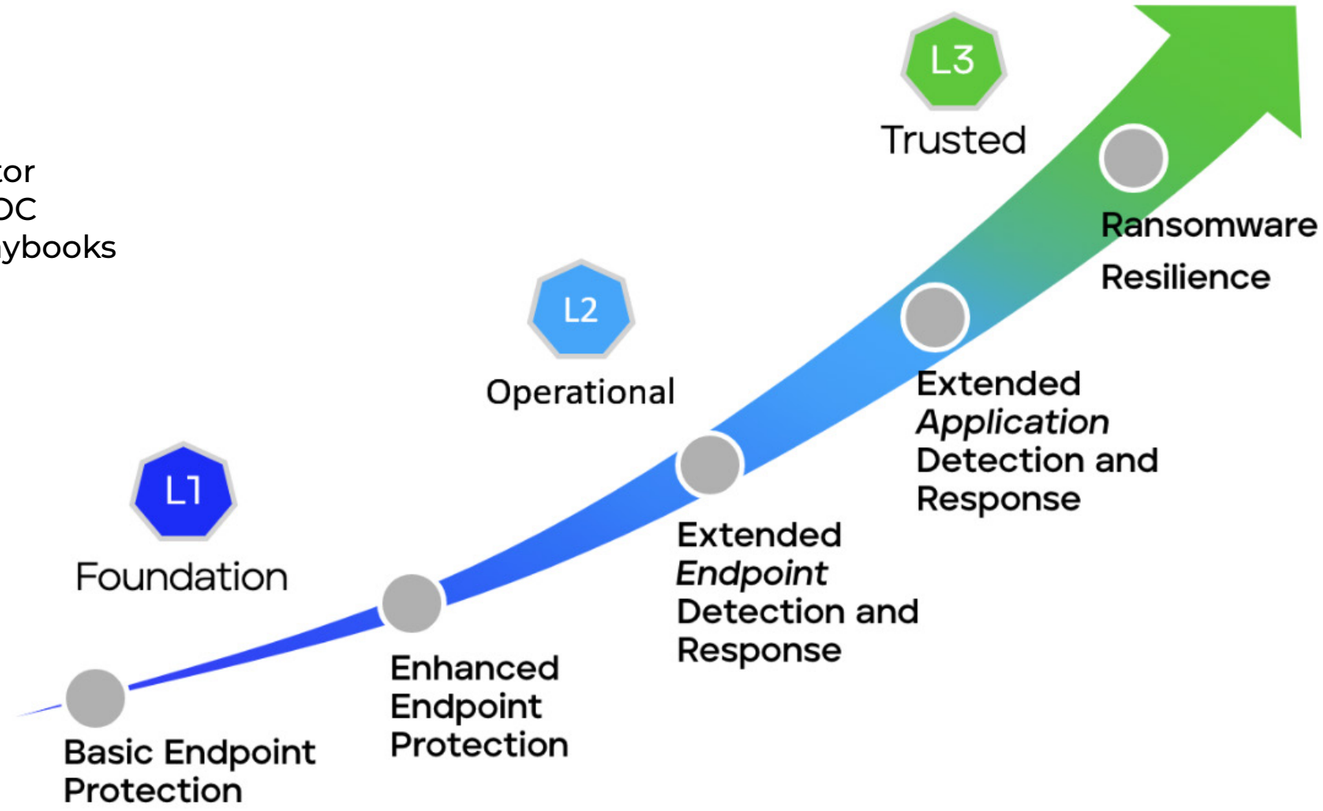
Level 2: Operational

Organizations at this level have implemented multi-vector prevention, detection and response. At this level, your SOC is more proactive than reactive, and has a number of playbooks to help guide response.

Level 3: Trusted

At this level, organizations are adaptable. You conduct regular exercises and assessments. You've evolved from reactive to predictive. Your SOC knows what is going to happen based on what it is seeing.

Every organization is different. An engagement with professional services can go much deeper to assess readiness, identify gaps, and create a plan that is tailored for your organization.



ACCELERATE RANSOMWARE DETECTION AND RESPONSE WITH THE TRELLIX XDR PLATFORM

One of the best ways to gain visibility at any stage of an attack is with an extended detection and response (XDR) solution that provides multi-vector detection and faster context. The Trellix XDR Platform offers AI-powered speed when every minute matters:

Comprehensive native controls: One platform of best-of-breed tools to replace five or more point products

Integrated analyst experience: Dashboards designed by analysts, for analysts, and playbook automation to enrich data and remediate threats

Multi-vector threat detection: Turn event noise from multiple controls into prioritized, insightful actions

Open platform: More than 500 out-of-the-box integrations for quick time to value

Actionable threat intelligence: Operationalize threat intelligence from 1 billion global sensors to produce actionable, real-time insights on emerging threats

Future proof investment: AI-powered, scalable hybrid architecture grows with your environment and as new technologies emerge

TAKE THE NEXT STEP

Request a custom demo for your organization.

Learn more with these resources

Trellix Solution for Ransomware Detection and Response

Trellix XDR Platform

Trellix Ransomware Detection and Response Virtual Showcase

Visit Trellix.com to learn more.

About Trellix

Trellix is a global company redefining the future of cybersecurity. The company's open and native extended detection and response (XDR) platform helps organizations confronted by today's most advanced threats gain confidence in the protection and resilience of their operations. Trellix's security experts, along with an extensive partner ecosystem, accelerate technology innovation through machine learning and automation to empower over 40,000 business and government customers.