Deloitte.
デロイト トーマツ

Deloitte Cyber Incident Handling

Ransomware Readiness Program

February 2023

Contents

If you know the enemy an know yourself, you need not fear the result of a hundred battles.

What is Ransomware?

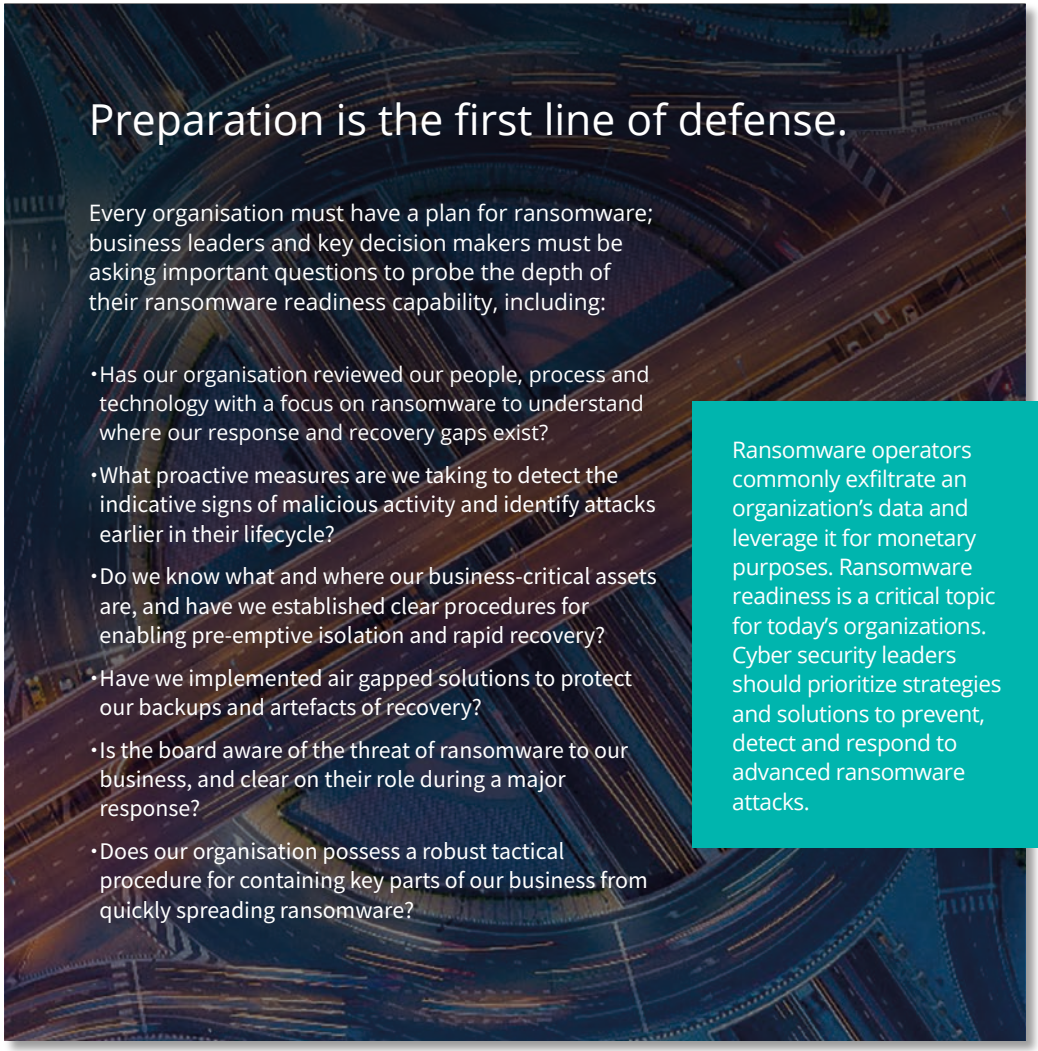
Ransomware is a type of malware that encrypts a victim's files and demands a ransom payment in exchange for the decryption key. Ransomware attacks can cause significant disruption and financial loss for organizations. It can also spread through networks, encrypting multiple computers and making it more difficult and expensive to recover the encrypted files.

What is a Ransomware Attack?

A ransomware attack is an incident in which a organization’s files are encrypted and a ransom is demanded for the decryption key. The attack typically begins with the victim unknowingly downloading and installing the ransomware, often through a phishing email or an infected website. Once the ransomware is installed, it encrypts the victim's files, making them inaccessible. The attacker then demands a ransom payment, usually in a cryptocurrency, in order to provide the victim with the decryption key.Targets of ransomware attacks range from individuals to companies, but in the case of companies, the disruption to the continuity of business operations itself is sometimes the target of an attack. The damage caused by ransomware can be extensive, making it important for organizations to take proactive steps to protect themselves, such as implementing effective cybersecurity measures and business continuity plans.

Our company's anti-ransomware program

Our Cyber Intelligence Center (CIC) provides continuous monitoring of critical systems and networks of global clients 24 hours a day, 365 days a year to monitor for potential threats, such as ransomware, intrusion attempts, and malicious network activity. CIC has a team of security experts available to respond to any potential threats that are detected in real-time. They work with our clients to contain and neutralize the threat as quickly as possible.Our incident response team specialists have significant experience and expertise in identifying, assessing, and responding to ransomware attacks, and can help organizations minimize the impact of such an attack and recover their systems and data.Our offensive security team simulate advanced ransomware attacks to help organizations identify security issues, potential attack paths and improve their ransomware response capabilities. Sun Tzu famously said, " If you know the enemy and know yourself, you need not fear the result of a hundred battles. " This important quote is working considering when developing a ransomware strategy and countermeasures.Our company is leading the battle against ransomware. We can help your organization, too.



Recovering from a ransomware infection. Why it remains a challenge

01 Ransomware-as-a-service (RaaS) and ransomware access brokers have made it easier for individuals or groups without significant technical skills to launch ransomware attacks, making ransomware a growing trend in the cybercrime world.

02 Ransomware recovery time can range from a few hours to several weeks. Long system recovery increases the overall cost of recovering from a ransomware attack. Additionally, there are indirect costs such as lost productivity, lost revenue, damage to reputation and brand, legal and regulatory fines and compensation for affected customers. Estimates place the average cost of ransomware recovery at around $1 million USD.

03 The overhaul of cyber insurance industry and ransomware coverage coupled with the increased regulation of ransom payments across the globe, means that organizations cannot always depend on insurance to mitigate the financial impact of a ransomware attack.

04 Double extortion ransomware attacks encrypts and organization's data while simultaneously exfiltrating sensitive data, threatening to release the data publicly if the ransom is not paid.

05 Ransomware is a continuously and rapidly evolving threat. New types and variants of ransomware are being developed all the time. This makes it difficult for businesses to protect themselves against all possible threats.

06 Active Directory is a widely used technology and a critical component of most organizations, making it an attractive target for ransomware attacks. Implementing sufficient ransomware protection mechanism and defenses across an entire Active Directory estate is a challenge for most organizations.

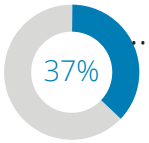
The reality of ransomware

Ransomware continues to be the most pervasive, destructive and costly cyber threat to organisations globally. Over the past twelve months there has been a distinct shift in the cybercriminal ecosystem, with changes in the tactics employed by threat groups resulting in a marked increase in attacks and the "professionalisation" of the ransomware business model.

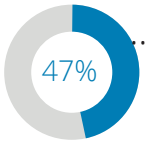
Ransomware adversaries are becoming more discerning, shifting their focus away from the Big Game Hunting (BGH) tactics that have long dominated the cyber threat landscape. Threat groups have instead reverted back to opportunistic and indiscriminate targeting of businesses, leveraging the lessons learned from BGH campaigns. This change in tactic has resulted in a higher proportion of payments while also avoiding the scrutiny of government and law enforcement which high profile attacks against larger corporations tend to attract.

Hybrid attacks with multiple layers of extortion have also become the new normal, with data theft and employee harassment now as engrained in ransomware operations as the encryption of ransomware itself. The lucrative and fast pay-off of this model has made these types of hybrid coercion attacks increasingly attractive to cybercriminals and ransomware affiliates, presenting distinct regulatory, financial and technology challenges for organisations.

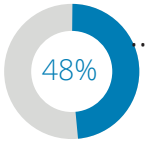
Ransomware statistics for the past 12 months



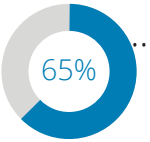
Organizations have experienced ransomware attacks



Recognize that stopping ransomware is increasingly difficult



Consider ransomware protection



Business leaders see inadequate ransomware as the biggest risk

Ransomware Readiness Program

Deloitte Tohmatsu Cyber's Ransomware Readiness Program is designed to help organizations protect themselves from sophisticated ransomware attacks. The program includes a comprehensive assessment of the critical, detection, response, and recovery capabilities of your organization.

Through our deep understanding of ransomware threats, their methods of infection and spread, and the impact that they have on organizations, we collaborate with our clients to develop and imple-ment effective security measures, processes, and training to mitigate ransomware threats.

We provide practical ransomware training, including information on the latest ransomware trends and techniques used by attackers, as well as guidance on how to recover from a ransomware attack. The goal of practical training is to empower individuals and organizations to protect themselves from this increasingly common and damaging form of cybercrime.

Our Ransomware Readiness Program has been developed by best-in-class security experts across Deloitte's expansive global network. The program includes several services that are designed to be adaptable and customizable, allowing organizations to benefit regardless of their level of maturity.

- Ransomware Readiness Assessment
- Attack Surface Management Assessment
- Incident Response Playbook Development
- Adversary Simulation Exercise

Our Approach

Deloitte's Ransomware Readiness Programme is designed to establish a global standard ransomware response and recovery capability, through an assessment of your current maturity, enhancement of your processes and procedures, and validation of your response capabilities.

The program is delivered in four phases:

01

Phase 1: Ransomware Readiness Assessment

Assess the detection and prevention security controls and incident response procedures of your organization.

02

Phase 2: Attack Surface Management Assessment

Attack Surface Management (ASM) is the process of identifying, alerting on, and mitigating vulnerabilities in an organization's internet facing systems and networks. The goal of ASM is to reduce the potential attack surface of an organization, making it less likely for attackers to successfully penetrate its defenses.

03

Phase 3: Incident Response Playbook Development

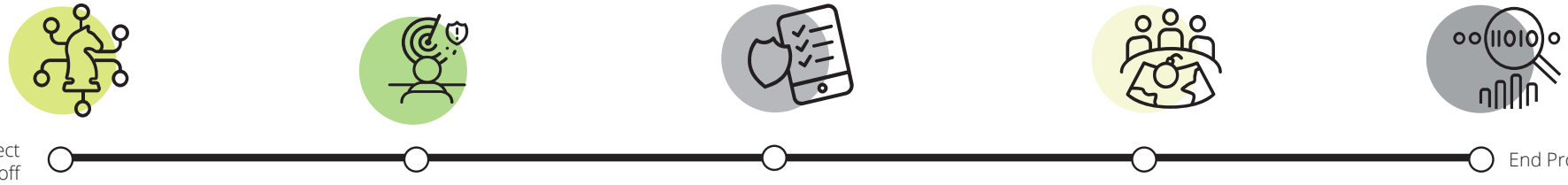
Ransomware incident response playbook development is the process of creating a step-by-step guide that outlines the procedures and actions to take in the event of a ransomware attack.

04

Phase 4: Adversary Simulation Exercise

Our ransomware adversary exercise is a simulated ransomware attack that is designed to test an organization's incident response plan, procedures, and readiness for dealing with a real-life ransomware attack. Using real world techniques, tactics and procedures (TTPs), we will simulate a ransomware attack in the organization's environment.

Program Flow and Expected Outcomes.



Phase 1
Ransomware Readiness Assessment

✓ We will better understand your current state, identify where you are vulnerable to ransomware, and design your future state roadmap for improving resilience

Phase 2
Attack Surface Management

✓ Identifying, alerting on, and mitigating vulnerabilities in an organization's internet facing systems and networks. Document potential ransomware attack vectors.

Phase 3
Playbook Development

✓ We will build you an end-to-end ransomware playbook to standardise your organisations response to and recovery from a ransomware incident

Phase 4
Simulation

✓ We will help you prepare for a ransomware incident by rehearsing your ability to respond to an attack, ensuring your people are clear on their role during a major response

Options
Options Threat Security Monitoring for EDR

Deloitte Cyber Intelligence Center provides 24/365 oversight to enhance your organization's EDR oversight.

01	02	03	04	05	06	07	08	09	10	11	12
Review Current State	Understanding Existing Capabilities	Identify Gaps and Weaknesses	Investigate risks and attack vectors in public facing systems	Review ransomware response procedures	Build Tactical Procedures	Dry run, verification of procedures	Facilitate and Observe	Ransomware awareness session	Design Ransomware Attack Scenarios	Ransomware Attack Simulation	Observe. Validate. Optimize

Readiness Assessment

Our framework for ransomware readiness is informed by operational experience on the front lines of ransomware incidents, and is aligned to the NIST Profile for Ransomware Risk Management along with industry leading practice published by the National Cyber Security Centre (NCSC).

Our experiences in supporting organisations who have been devastated by ransomware over the years have identified two insurmountable truths: that every organisation is a potential target, and that while the initiation of an attack may differ, the ransomware story is always the same. That story is, that an attacker will achieve a foothold within the network and will progressively move laterally and harvest credentials until achieving the desired level of privilege to achieve their objectives.

There is no single vulnerability which causes ransomware; rather, ransomware is an entire lifecycle challenge, with a string of weaknesses, exploits and adversary techniques comprising the wider ransomware "kill chain". Importantly, it is often the same control gaps and poor cyber hygiene practices which fail to protect against an intrusion, detect attacks earlier in their lifecycle, and enable efficient management of response and recovery efforts.

A clean line of sight.

Deloitte's Ransomware Readiness Framework is designed to provide organisations with a practical and achievable set of security principles which clearly articulate the critical capabilities and controls required to "break the kill chain" and defend against attacks, and to empower organisations to make more informed decisions around managing ransomware risk.

1 Harden the perimeter to prevent intrusion

- Web Filtering
- Email Filtering and Security
- Remote Services and Perimeter Access
- Media and Devices
- Security Monitoring and Intelligence

2 Secure Endpoints to Constrain Execution

- Application Control
- Macro Security and Scripting
- Vulnerability Management
- Remote Administration
- Anti-virus and Anti-malware
- Endpoint Detection and Response

3 Limit The Attack Radius

- Identity and Access Management
- Network Segmentation
- Firewalls and Assurance
- Active Directory
- Credential Protection
- Endpoint Configuration and Hygiene

4 Backup and Recovery

- Data Protection and Segregation
- Backup Integrity and Testing
- Recovery Planning and Resilience

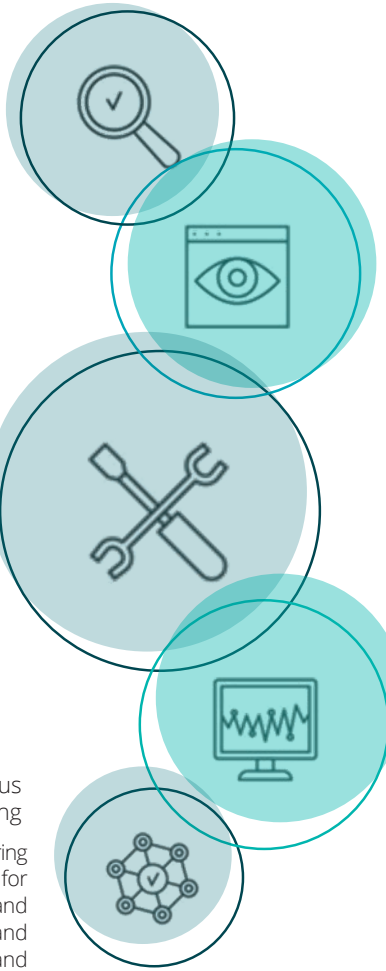
5 Cyber Incident Response

- Cyber Wargaming and Exercising
- Incident Management and Governance
- Policies, Procedures and Standards
- Burst Capacity

6 Ransomware Awareness Training

- Core Response Team Training
- Training for General Staff
- Awareness-raising Activities

How it works



Identify Perimeter Assets

identifying and inventorying all assets and systems that make up the organization's attack surface.

Information Gathering

Gather information from identified devices.

Analysis and Assessment

Analyzing the attack surface to identify potential vulnerabilities and risks. Prioritizing the identified vulnerabilities and risks based on the likelihood and impact of a successful attack.

Implement Countermeasures

Implementing controls and countermeasures to reduce the risk of a successful attack, such as patching vulnerabilities, configuring security settings, and implementing security monitoring.

Continuous Monitoring

Continuously monitoring the attack surface for new threats and vulnerabilities, and updating controls and countermeasures as necessary.

Attack Surface Management

Our Attack Surface Management (ASM) service uses publicly available information assess the external perimeter and the attack surface of your organization.

Overall, ASM information collection is a crucial step in identifying and managing potential vulnerabilities in an organization's systems and infrastructure, reducing the organization's attack surface and improving their overall security posture.

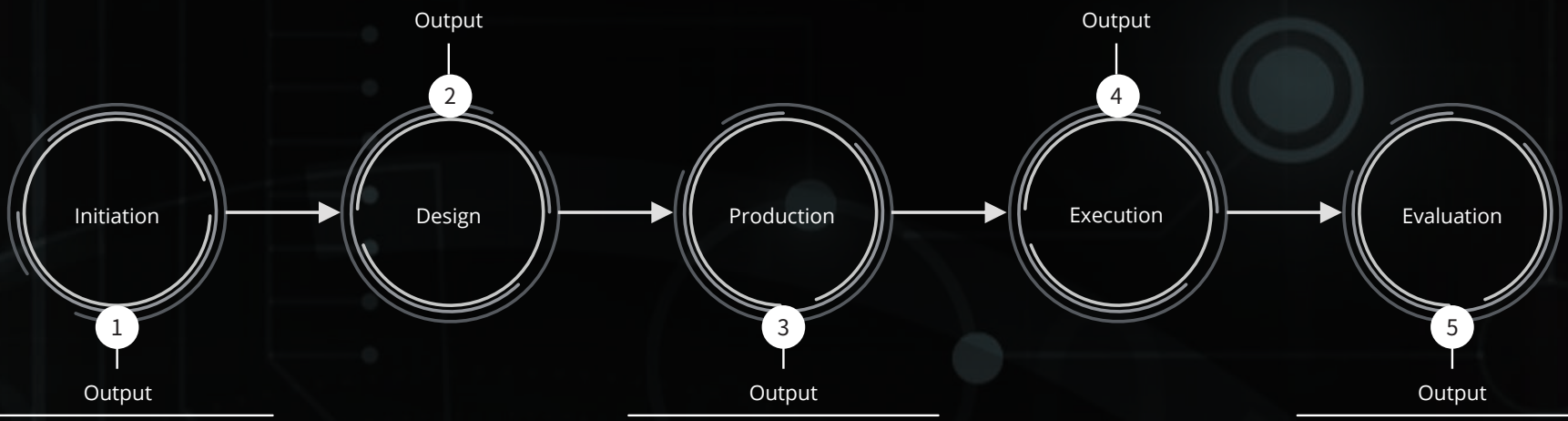
Information is collected entirely from a black box perspective using external publicly available information sources, without relying on internal information such as the client's IT asset inventory. In the case of ransomware attacks, devices such as VPN servers, which were quickly deployed to expand telework, became entry points for ransomware. ASM will provide a clear visibility of these assets, identifying potentially vulnerable targets for ransomware attackers.

Perimeter Risk Assessment

Attackers can use vulnerabilities in internet connected, perimeter assets to gain access to an organization's network and deploy ransomware. Organizations should ensure that these assets are configured and secured properly. This includes regularly patching and updating the firmware and software on these devices, and implementing strong authentication methods, such as two-factor authentication. Organizations should also regularly review and audit their perimeter device configurations and monitor for signs of unauthorized access.

A closer look at ransomware adversary emulation

Intelligence will be used to profile your threat landscape and prioritise the adversaries most likely to target you: this will allow us to select a suitable adversary to emulate. We will use the adversary's tactics, techniques, and procedures (TTPs) to build a kill-chain of technical tests mapped to MITRE ATT&CK. Each test will be executed to emulate a non-obtrusive, real-world attack, and identify any weaknesses in detection and prevention controls.



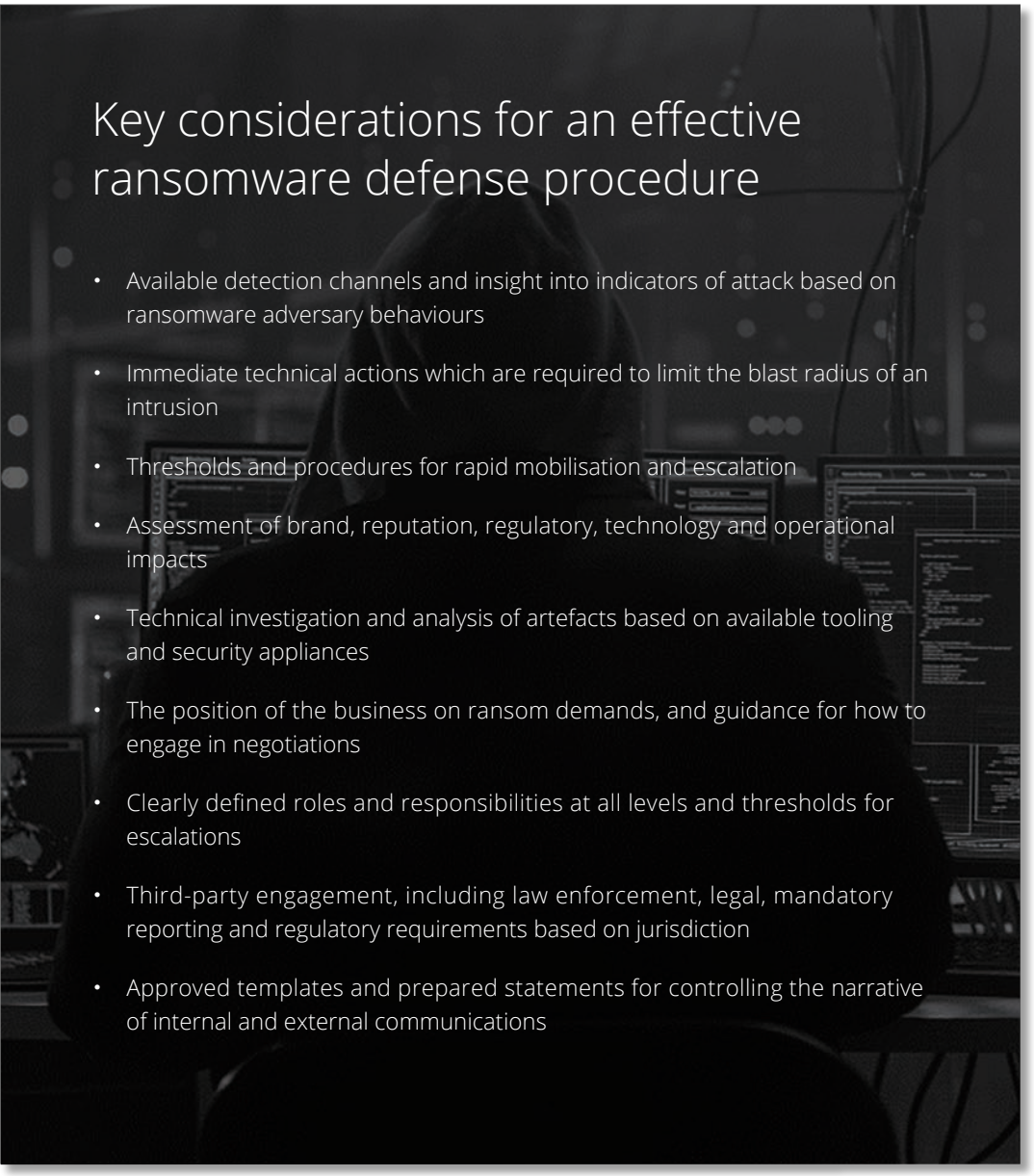
- Detailed threat profile and intelligence on the chosen adversary
- Programme overview, including objectives, scope and success criteria
- Pre-briefing sessions and emulation workshops diarised

- Tactics, Techniques and Procedures captured
- High-level scenario overview
- Detailed simulation scenario workflow
- Technical requirements for emulation activity

- Emulation plan detailing technical execution procedure(s)
- Participant pre-briefing packs, including objectives, tests to be run, validation guidance, assumptions, and success criteria
- Agent deployed to chosen infrastructure
- Detailed field manual outlining rules of engagement

- Technical team and facilitator briefing
- Execution of the emulation scenario
- Validation of results against success criteria
- Tactical refinement of tooling and detection processes

- Debrief meetings held with key stakeholders
- Post-emulation report identifying results from each test, tactical control enhancements and strategic process improvements
- Agent and artefact clean-up



Key considerations for an effective ransomware defense procedure

- Available detection channels and insight into indicators of attack based on ransomware adversary behaviours
- Immediate technical actions which are required to limit the blast radius of an intrusion
- Thresholds and procedures for rapid mobilisation and escalation
- Assessment of brand, reputation, regulatory, technology and operational impacts
- Technical investigation and analysis of artefacts based on available tooling and security appliances
- The position of the business on ransom demands, and guidance for how to engage in negotiations
- Clearly defined roles and responsibilities at all levels and thresholds for escalations
- Third-party engagement, including law enforcement, legal, mandatory reporting and regulatory requirements based on jurisdiction
- Approved templates and prepared statements for controlling the narrative of internal and external communications

Playbook Development

Our ransomware playbooks, emphasising both technical teams and executive leadership, are designed to provide you with clear and practical guidance, detailed response actions and key considerations for responding to and recovering from a ransomware incident, allowing you to mobilise quickly and act decisively when confronted with the impacts of an attack.

Organisations who have well-thought-out, well-defined plans for responding to cyber threats, and continually iterate these plans factoring in changes to their threat landscape and business environment, avoid common pitfalls and panic-driven decision-making, resulting in much quicker, more decisive, and more cost-efficient responses.

We will design and deliver a ransomware playbook which standardises response procedures, decision-making and technical actions across your organisation, enabling you to coordinate a swift and effective whole-of-business response to a ransomware incident. Our ransomware playbook is designed with versatility in mind, ensuring you are equipped with the information you need to respond to all possible permutations and eventualities of a ransomware attack.
Importantly, we will incorporate key learnings from our readiness assessment based on our understanding of your existing capabilities and blind spots. This will allow us to define practical technical processes, fail-safes and critical response considerations which address the most likely ransomware attack scenarios and prominent exposures in your environment.

Respond with confidence

Our playbooks are aligned to the National Institute of Standards and Technology (NIST) Computer Security Incident Handling guidelines, following an industry recognised methodology which is constructive, adaptable, and impactful.

- TECHNICAL ACTIONS REQUIRED TO INVESTIGATE, CONTAIN AND RECOVER FROM AN INCIDENT
- INCIDENT REPORTING REQUIREMENTS AND YOUR RESPONSIBILITIES TO REGULATORS
- THE ROLE OF YOUR PEOPLE DURING A RESPONSE, FROM ALL CORNERS OF THE BUSINESS
- INCIDENT HANDLING GUIDANCE TO MANAGE STRATEGIC AND OPERATIONAL IMPACTS

Ransomware Adversary Emulation

Ransomware Adversary Emulation provides a real-world evaluation of your detection and prevention capabilities through objective-based technical simulations derived from behaviours and techniques used by ransomware adversaries.

Our Ransomware Adversary Emulation service will allow you to verify assumptions in your security posture and validate defensive capabilities in practice to quantify the effectiveness of your controls and processes against destructive cyber-attacks.

Our specialists will design and deliver a series of proactive technical simulations based on real-world adversaries to validate your technical cyber security controls and document their effectiveness in detecting and preventing emulation activity.

In doing so we will identify any control gaps and weaknesses to drive improvements in your cyber posture, achieve greater visibility of adversary tradecraft, and enhance your ability to detect and prevent ransomware behaviours earlier in their lifecycle.

Key benefits of recreating ransomware campaigns

01

Understand how effective your defensive capabilities are in preventing and detecting ransomware attacks before an incident

02

Gain insight into novel ransomware adversary techniques which can evade your security controls and defences

03

Identify essential control enhancements and countermeasures to defend against ransomware

Simulation Flow

1

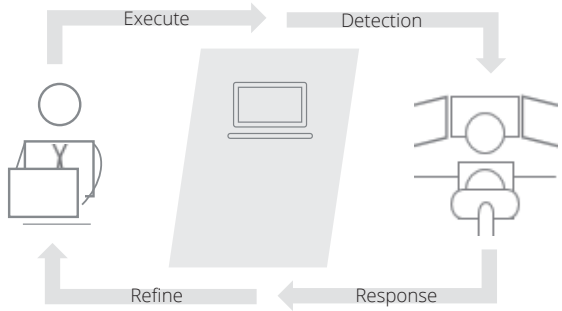
Pre-Briefing

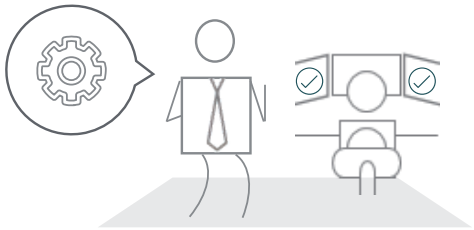
Deloitte facilitators will deliver a dry-run of the activity, highlighting objectives, success criteria, tests to be performed, and guidance for validation

2

Adversary Simulaton

Deloitte SMEs will execute a series of technical tests based on the agreed adversary scenario to validate the effectiveness of detection and prevention capabilities





3

Reporting

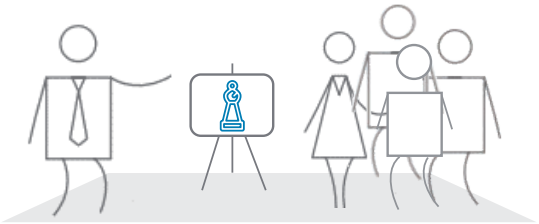
Deloitte will propose tactical enhancements for improving detection and prevention based on the results of the simulation

Ransomware Awareness and Exercising

Anatomy of a tabletop exercise

1 Pre-Briefing

Deloitte facilitators will deliver a dry-run of the activity, highlighting exercise guidance, rules of play and context on the given scenario to exercise participants

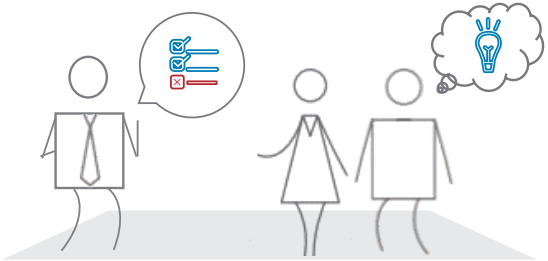


2 Exercise

The control team and facilitators will coordinate scenario progression, delivering scenario injects and attacks, while monitoring discussion, decisions and progress

3 Lessons Learned

Deloitte will review exercise outcomes and collect participant feedback to identify what worked well, and where improvements can be made



Our Ransomware Awareness and Exercising service is designed to support you in building a deeper understanding of the threat of ransomware, through rehearsing and validating the response of your people against an end-to-end ransomware scenario

Cyber Wargames are functional exercises where participants are prompted to make strategic decisions and focus on the 'what if'. These exercises provide an opportunity to rehearse, make mistakes and fundamentally learn in an environment free from direct consequences, leading to broader consensus of the appropriate strategies and activities to execute during a real response.

How would your organisation respond to ransomware?

Our team will design and facilitate a tabletop exercise based on a realistic ransomware scenario, tailored specifically to your technology estate and business environment, and which focuses on the threats most relevant to your business. This will allow us to observe the response and decision making of your business leaders and technology teams, understand pain points and familiarity with existing processes, and capture lessons learned for improving your ability to respond.

Lessons learned from the front lines

Our enterprise response and recovery specialists will share observations from the front lines of ransomware, highlighting the realities of a breach, visibility into modern ransomware threat actor playbooks, attack vectors and tradecraft, and insight into where organisations often "miss the mark", enabling you to learn from the lessons of others.

Bringing our ransomware expertise to bear

Our proposed team has been carefully selected based on an intimate understanding of the cyber risks facing the sector, and extensive operational experience in supporting organisations to prepare for and recover from ransomware attacks.

Our team know ransomware, and are proven leaders in building ransomware resilient organisations, uniquely positioning us as the right partner to assist you in evaluating and enhancing your ability to detect, respond and recover.

Project Quality Assurance | Support engagement excellence

Partner
Kohei Sato
Mail: kohei.sato@tohmatsu.co.jp

Partner
Ari Davies
Mail: ari.davies@tohmatsu.co.jp

Managing Director
Akinori Toriyabe
Mail: akinori.toriyabe@tohmatsu.co.jp

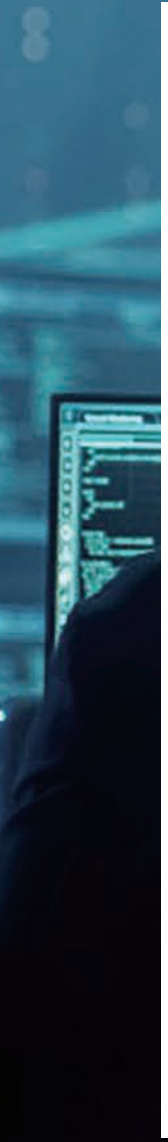
Managing Director
Kenichi Inoue
Mail: kenichi.inoue@tohmatsu.co.jp

Project Leadership | Delivering the exceptional value you expect

Director
Tadashi Oba
Mail: tadashi.oba@tohmatsu.co.jp

Manager
Robert Dracea
Mail: robert.dracea@tohmatsu.co.jp

Specialist Leader
Barry O'Callaghan
Mail: barry.ocallaghan@tohmatsu.co.jp



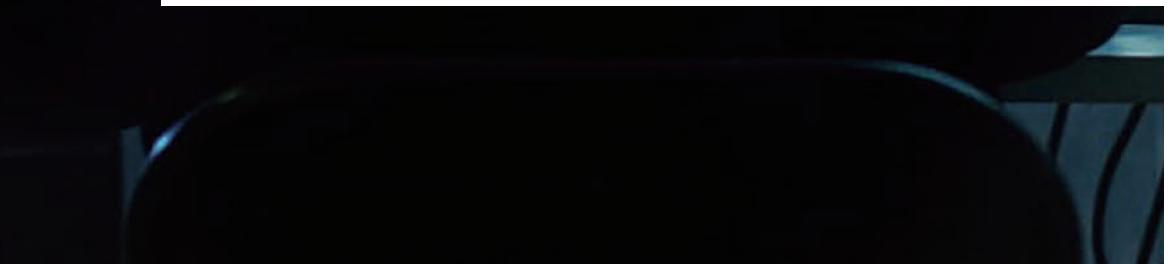
Value Delivered

01 Deloitte initially deployed technical responders to support early triage and analysis of the incident before deploying various skill sets to wider operational locations around the world, resulting in over 200 Cyber, IT Recovery and Crisis Response staff deployed within a 9-day period.

02 Deloitte secured a key piece of network infrastructure that expedited recovery and begun the process of recovering and rebuilding a global network of over 8,000 servers, 60,000 end points and 1 million+ applications.

03 During the technical response and recovery, Deloitte assisted the client in developing a short-, medium- and long-term cyber recovery and transformation plan to improve their overarching cyber security posture.

04 Our support enabled the client to recover into the future rather than the past, saving money and expediting their cyber transformation journey.



Case Study: Ransomware Response and Recovery

Our client, a renowned shipping company, engaged Deloitte to support the recovery of their business following a major ransomware incident that had crippled their global operations.

Services provided

- Incident Management and Coordination
- Active Directory Architect
- Enterprise Recovery Specialist
- Cyber Threat Intelligence
- Survey Support
- eDiscovery
- Communications
- Malware Analysis

Case Study: Anti-Ransomware Program

Our client is a multinational investment bank; their objective was to achieve greater resilience against the threat of ransomware through building a global standard response and recovery capability across the business

Services provided

- Ransomware Subject Matter Experts
- Ransomware Readiness Assessment
- Tactical Procedures (Playbook)
- Ransomware Awareness Session(s)
- Cyber Drill(s)
- Ransomware Tabletop
- Remediation Planning
- After-Action Report(s)

Value delivered

01 Deloitte performed a Ransomware Readiness Assessment to assess the client's current control maturity across their global business, and to identify where the client is vulnerable to ransomware.

02 Deloitte identified inherent weaknesses in the client's endpoint hygiene and cyber posture which had remained undetected, and which exposed the client to compromise, and proposed tangible recommendations and security enhancements to reduce their attack surface.

03 Leveraging the visibility achieved through the assessment, Deloitte developed a ransomware tactical procedure (playbook) which standardised response and recovery actions for the Global Cyber Security Incident Response Team.

04 Our team facilitated a programme of ransomware training sessions, drills and tabletop exercises to enshrine awareness of new processes and capabilities, and to rehearse and validate the client's response to an end-to-end ransomware scenario.

05 Our support enabled the client to better understand the threat of ransomware, remediate critical weaknesses in their environment, secure essential investments for improving resilience to ransomware, and demonstrate their readiness to respond to the executive committee.

Recognized leaders in cyber incident response

#1 in Security Consulting Services by market share for the eleventh consecutive year
(Gartner, report titled, Market Share: Security Consulting Services, Worldwide, 2021)

https://www2.deloitte.com/global/en/pages/about-deloitte/-press-releases/for-the-eleventh-consecutive-year-deloitte-retains-its-no-1-position-in-security-consulting-services-by-market-share.html

Worldwide leader in IDC MarketScape for Worldwide Incident Readiness Services
(IDC MarketScape: Worldwide Incident Readiness Services 2021 Vendor Assessment)

https://www2.deloitte.com/global/en/pages/about-deloitte/-press-releases/deloitte-named-a-worldwide-leader-in-idc-market-scape-for-worldwide-incident-readiness-services.html

Leader in The Forrester Wave™: Cybersecurity Incident Response Services, Q1 2022.
(The Forrester Wave™: Cybersecurity Incident Response Services, Q1 2022)

https://www2.deloitte.com/global/en/pages/technology/articles/cybersecurity-incident-response-services.html

Global leader in Cybersecurity Consulting by ALM
(The ALM Vanguard: Cybersecurity Consulting 2019)

https://www2.deloitte.com/global/en/pages/about-deloitte/-press-releases/deloitte-recognized-global-leader-in-cybersecurity-consulting-by-alm.html

Deloitte.
デロイト トーマツ

Deloitte Tohmatsu Group (Deloitte Japan) is a collective term that refers to Deloitte Tohmatsu LLC, which is the Member of Deloitte Asia Pacific Limited and of the Deloitte Network in Japan, and firms affiliated with Deloitte Tohmatsu LLC that include Deloitte Touche Tohmatsu LLC, Deloitte Tohmatsu Consulting LLC, Deloitte Tohmatsu Financial Advisory LLC, Deloitte Tohmatsu Tax Co., DT Legal Japan, and Deloitte Tohmatsu Corporate Solutions LLC. Deloitte Tohmatsu Group is known as one of the largest professional services groups in Japan. Through the firms in the Group, Deloitte Tohmatsu Group provides audit & assurance, risk advisory, consulting, financial advisory, tax, legal and related services in accordance with applicable laws and regulations. With approximately 17,000 people in about 30 cities throughout Japan, Deloitte Tohmatsu Group serves a number of clients including multinational enterprises and major Japanese businesses. For more information, please visit the Group's website at www.deloitte.com/jp/en.

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited ("DTTL"), its global network of member firms, and their related entities (collectively, the "Deloitte organization"). DTTL (also referred to as "Deloitte Global") and each of its member firms and related entities are legally separate and independent entities, which cannot obligate or bind each other in respect of third parties. DTTL and each DTTL member firm and related entity is liable only for its own acts and omissions, and not those of each other. DTTL does not provide services to clients. Please see www.deloitte.com/about to learn more.
Deloitte Asia Pacific Limited is a company limited by guarantee and a member firm of DTTL. Members of Deloitte Asia Pacific Limited and their related entities, each of which are separate and independent legal entities, provide services from more than 100 cities across the region, including Auckland, Bangkok, Beijing, Hanoi, Hong Kong, Jakarta, Kuala Lumpur, Manila, Melbourne, Osaka, Seoul, Shanghai, Singapore, Sydney, Taipei and Tokyo.

Deloitte provides industry-leading audit and assurance, tax and legal, consulting, financial advisory, and risk advisory services to nearly 90% of the Fortune Global 500® and thousands of private companies. Our professionals deliver measurable and lasting results that help reinforce public trust in capital markets, enable clients to transform and thrive, and lead the way toward a stronger economy, a more equitable society and a sustainable world. Building on its 175-plus year history, Deloitte spans more than 150 countries and territories. Learn how Deloitte's approximately 415,000 people worldwide make an impact that matters at www.deloitte.com.

This communication contains general information only, and none of Deloitte Touche Tohmatsu Limited ("DTTL"), its global network of member firms, or their related entities (collectively, the "Deloitte organization") is, by means of this communication, rendering professional advice or services. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser. No representations, warranties or undertakings (express or implied) are given as to the accuracy or completeness of the information in this communication, and none of DTTL, its member firms, related entities, employees or agents shall be liable or responsible for any loss or damage whatsoever arising directly or indirectly in connection with any person relying on this communication. DTTL and each of its member firms, and their related entities, are legally separate and independent entities.

Member of
Deloitte Touche Tohmatsu Limited

IS 669126 / ISO 27001

BCMS 764479 / ISO 22301