SECURITY CONSULTING SERVICES

Incident Response and Forensics

Are you prepared for a security incident?

In today's complex threat landscape no one is immune from cyber attacks and data breaches, and organizations increasingly understand that planning for security incidents is an essential element in their business strategy. Today, how well you respond to an incident has a direct bearing on reputation, share price, and business success.

Incident response planning isn't just about good sense, it is also a requirement of the EU General Data Protection Regulation (GDPR) and the Network and Information Systems Regulations (NIS Regulations). Both regulations require organizations to maintain a high level of information security, report breaches in a timely manner, and explain the steps taken to prevent future attacks.

While incidents are increasing in frequency, businesses are spending more time and money on remediation. And the maturity of incident response varies considerably, with high-performing businesses treating information security breaches as part of their business continuity planning.

Not all incidents are equal

To confidently answer this question, you have to first know that you are under attack by establishing a comprehensive, real-time view of network activity. You can then implement a clear plan for the right remedial action for your business. Not all incidents are equal, so it's important to be able to classify the impact of the incident. This will drive a proportionate response and focus resources to minimize damage and disruption, returning to business as usual as quickly and smoothly as possible.

Good incident response therefore starts with good risk insight and an understanding of your information assets. But this does not necessarily mean spending more on technology.

Organizations can lack clarity around incident response processes, the skills they require in their existing team to manage an incident, and who they would turn to for help in the event of a breach. Furthermore, organizations rarely have spare resources waiting to leap into action when an incident happens, which is why they may seek a trusted partner if the worst happens.

Understanding compliance

It is vital to understand where compliance fits into your incident response processes and have a clear procedure in place to meet your specific obligations for reporting incidents.

We help NTT clients to put processes in place to ensure they know when and how to notify law enforcement or specific industry regulators.

This involves establishing policies with other parts of the business affected by a breach. And the introduction of GDPR and NIS Regulations means that organizations now need to notify breaches soon after discovery, along with the measures taken to manage the breach and the steps taken to prevent future incidents from occurring.

Benefits of our Security Incident Response and Forensics

Immediate Response – Threat Detection Incident reporting is used to trigger a team of incident responders

Minimizes impact of incidents – rapid incident identification will significantly limit the impact to your organization

Reduce costs – pre-negotiated rates mean that you will minimize the cost of the incident

Preserve critical evidence – particular care with forensic evidence is essential for law enforcement and legal action

Brand protection – careful management of the incident can substantially reduce brand damage

Meet risk and compliance goals – correct procedures ensure you meet regulatory compliance reporting requirements

Culture and collaboration

A security breach can naturally result in some finger pointing. We are used to having fire drills, but organizations do not always consider the value of using high-visibility exercises such as rapid-response communication drills and table top exercises – simulating potential incidents to improve awareness and define roles and responsibilities beyond the technology teams.

In our experience, these activities heighten the sense of joint responsibility for effective resolution.

Building the right incident response model

Not all companies are mature in their incident response planning and execution. We work with new and existing NTT clients to build a structured plan that clearly articulates the approach, benefits and measures for application risk reduction. But our work does not end here. Our breadth of experienced resources means that we also deliver the plan – only handing back to you when all test criteria are successfully met.

For organizations that understand the value of fast, efficient response, part of the plan can include the use of a specialist incident response team. Armed with a clear understanding of your business and technology infrastructure, this dedicated team would:

- Establish a presence at your organization
- Perform network and host-based forensic investigation into the incident
- Provide incident management capability
- Deliver a summary post-incident report and recommendations

Actions when an incident occurs

Our unique threat detection, advanced analytics, and unrivalled threat intelligence capabilities give you the convenience of being able to engage with one global provider for all your cybersecurity needs. The incident report is used as a trigger for our response services.

Incident Response can be delivered to you as part of NTT's Global Managed Security Services in combination with NTT Consulting Services. With many organizations struggling to manage all aspects of cybersecurity in-house, partnering with NTT gives you access to our world-class specialist organization and security experts.

Our Managed Security Services provide management of security devices which can act directly to update policies to block an attack. Our Endpoint Detection and Response (EDR) service quarantines affected endpoints to stop further spreading of verified malware.

Managed Security Service clients can also request NTT SOC analysts to take further response actions for validated security incidents, where responsibility for network threat containment is passed to the NTT SOC. The team will identify threats, contain them and take the appropriate responsive action on each incident to prevent the further progress of the attack.

NTT Consulting Services can provide critical security incident response and recovery capabilities in order to help our clients to quickly resolve crisis situations. The service is delivered with a combination of architecture and forensics specialists, acting remotely and/or on-site.

Figure 1: NTT Incident Response helps you to minimize the impact and cost of an incident, as well as protecting your valuable data, intelligently adapting to prevent further incidents.

INCIDENT OCCURS	NTT TEAM DEPLOYED	INCIDENT MANAGEMENT CAPABILITY ESTABLISHED	FORENSIC ANALYSIS AND INCIDENT CONTAINMENT	INCIDENT RESOLUTION	INCIDENT CLOSURE AND WRAP UP	INCIDENT REPORT AND ROADMAP
• You suffer incident and have no in-house capability	• NTT deploys a skilled, rapid response team to your site, including incident handlers and technical analysts	• We rapidly establish process structure to handle the incident on your behalf	• Our analysts investigate, identify, analyze and contain the cause of the incident	• We provide support, guidance and remediation action for you to resolve the incident	• We support the closure of the incident and wrap up on-site activities	• Post incident, NTT provides a report on the incident, along with a tactical road map of recommendations to reduce risk

About us

NTT is a leading, global technology services company. We believe that together we do great things. We've combined the capabilities of 28 remarkable companies to create one, leading technology services provider. Partnering with you, we empower your people, strategy, operations, and technology through our full range of unparalleled capabilities and services. Together we enable the connected future.

Want to know more about our range of security consulting services?

Visit **hello.global.ntt** for details.