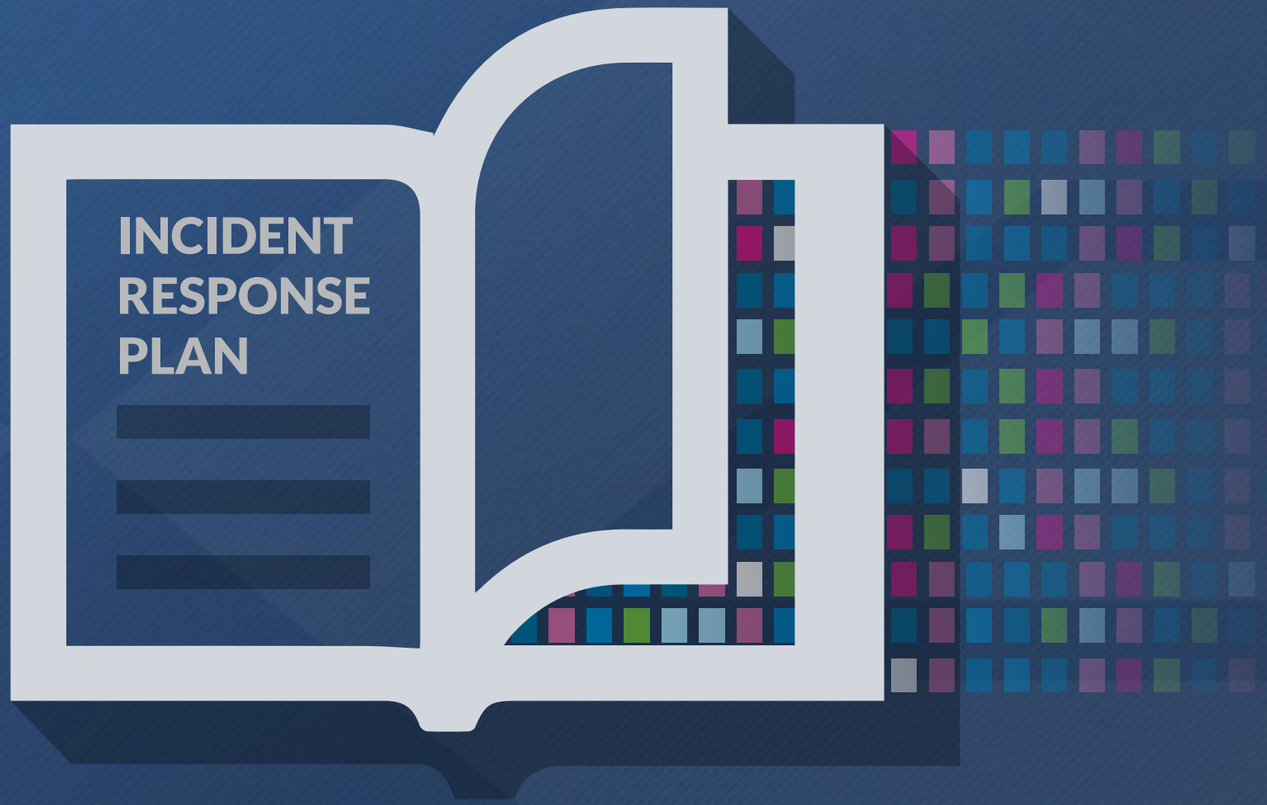
INCIDENT RESPONDER'S FIELD GUIDE

LESSONS FROM A FORTUNE 100
INCIDENT RESPONSE LEADER



DIGITALGUARDIAN®

TABLE OF CONTENTS

WHY READ THIS GUIDE?

Careful cyber security incident response planning provides a formal, coordinated approach for responding to security incidents affecting information assets. This e-book provides easy-to-follow steps for crafting an incident response plan in the event of cyber security attacks.

HOW TO USE THIS GUIDE

IF YOU ARE...	GO TO...
New to Incident Response Plan	Part One: Incident Response Do's and Don'ts
Not sure where to start?	Part Two: Get Ready
Familiar with Incident Response Plans, but how do I implement in my organization	Part Three: The Five Stages of Incident Response
Worried about managing Incident Response with limited resources	Part Four: Advanced Threat Protection as a Service
Looking to understand what makes Digital Guardian different	Appendix: Digital Guardian — Next Generation Data Protection

INCIDENT RESPONSE EXPERT

Tim Bandos is the Director of Cybersecurity at Digital Guardian. He has over 15 years of experience in the cybersecurity realm at a Fortune 100 company with a heavy focus on Internal Controls, Incident Response & Threat Intelligence. At this global manufacturer, he built and managed the company's incident response team.

Tim recently joined Digital Guardian to help build our Managed Security Program (MSP) to deliver advanced threat protection to our global customer base. He brings a wealth of practical knowledge gained from tracking and hunting advanced threats targeted at stealing highly sensitive data.

SEE OUR BLOG

· To learn why Tim joined Digital Guardian read his blog post, Why I Signed on with an IT Security Vendor.

TIM BANDOS
Director, Cybersecurity
Digital Guardian CISSP, CISA, CEH & CASS

DIGITALGUARDIAN®

PART ONE
INCIDENT RESPONSE DO'S AND DON'TS

5 THINGS **NOT** TO DO DURING AN INCIDENT

1 PANIC

Do **not** panic. It's the worst thing you can do. You want to remain calm and having an IR plan will help to do just that. An IR plan will provide you with a predefined path that outlines the best course of action to take during an incident.

2 SHUT DOWN SYSTEMS

Do **not** shut down infected systems. By shutting them down, you could lose volatile data that contains important forensic information. This information can be essential in determining the timeline of what transpired.

3 SOCIALIZE

Do **not** discuss the incident with others unless otherwise directed. It's important to be cautious about the audiences that you choose to communicate with about an incident that has just begun to unravel.

4 USE DOMAIN ADMIN CREDENTIALS

Do **not** use domain administrative credentials when accessing systems environment. Threat actors patiently wait for a user with enterprise-wide access to login in order to capture the password to gain complete control over the environment.

5 NON-FORENSIC TOOL USAGE

Do **not** execute any non-forensic software on the infected systems because this will overwrite the timelines associated with the attack in the Master File Table.

4 THINGS **TO DO** DURING AN INCIDENT

1 COLLECT DATA

Collect volatile data and other critical artifacts off the system using forensic tools.
Forensically sound tools have the ability to connect to the system without modifying any timestamps on the device.

2 EXTERNAL INTELLIGENCE

Gather external intelligence based on identified indicators of compromise (IOC). Search the web for intelligence about specific MD5s, IP addresses, domains that you discovered during your initial incident investigation. You are attempting to identify what the potential infection is or what type of malware may have been executed within the environment.

3 SAFEGUARD

Safeguard systems and other media for forensic collection.

4 COLLECT LOGS

Collect the appropriate logs. This may include Windows Events, Firewall, Netflow, Anti-Virus, Proxy, etc. It is important to view the story both at the network and at the endpoint level.

DIGITALGUARDIAN®

PART TWO
GET READY

BUILD YOUR IR TEAM

An Incident Response team is a centralized team that is responsible for incident response across the organization.

The team receives reports of security breaches, analyzes the reports and takes necessary responsive measures.
The team should be composed of:

INCIDENT RESPONSE MANAGER

IR manager oversees and prioritizes different steps in detection, analysis and containment of the incident. In case of high severity incidents, IR manager also interfaces with the rest of the company, including corporate security, human resources, etc. to convey findings, status, and requirements.

SECURITY ANALYSTS

These are the cyber-ninjas that go deep down into the weeds to identify when an incident has occurred and what has happened during that period of time. The team consists of:

- Triage Analysts - Filter out false positives and alert on potential intrusions
- Forensic Analysts - Recover key artifacts of data and maintain integrity of evidence to ensure a forensically sound investigation.

THREAT RESEARCHERS

Threat researchers complement security analysts by providing threat intelligence and context to the incident. They are constantly combing the internet, identifying intelligence that may have been reported externally. They then build an internal database of internal intelligence derived out of prior incidents.

GET CROSS-FUNCTIONAL SUPPORT

All business representatives must fully understand and advocate the Incident Response plan in order to ensure that the plan is properly executed, smooth information flow occurs and remediation takes place.

MANAGEMENT

Management buy-in is necessary for provision of resources, funding, staff, and time commitment for incident response planning and execution.

HUMAN RESOURCES

Human Resources is called upon when an employee is discovered to be involved with the incident.

AUDIT AND RISK MANAGEMENT SPECIALISTS

The specialists help develop threat metrics and vulnerability assessments, along with encouraging best practices across the constituency or organization.

GENERAL COUNSEL

The Attorney's role is to ensure the forensic value of any evidence collected during an investigation in the event that the company chooses to take legal action. An attorney can also provide advice regarding liability issues in the event that an incident affects customers, vendors, and/or the general public.

PUBLIC AFFAIRS

The Public Relations' role is to communicate with team leaders, ensuring an accurate understanding of the issue and the company's status, so as to communicate with the press and/or informing the stockholders about the current situation.

TIPS FROM TIM

TIM BANDOS
Director, Cybersecurity
Digital Guardian CISSP,
CISA, CEH & CASS

COMMUNICATION WITHIN AND ACROSS TEAMS IS CRITICAL

Communications during an incident should be conducted in a manner which protects the confidentiality of the information that is being disseminated. The incident response manager should be the central point of all communication and only those with a valid need-to-know is included in communications regarding key incident details, indicators of compromise, adversary tactics and procedures. Securing this communication so that Mr. Threat Actor is unable to snoop your messages is extremely vital to avoid tipping them off that an on-going investigation is occurring. Any indication that 'You're On to Them' may lead to swift changes by the attackers to further mask their activity.

WE HOPE YOU ENJOYED THIS SAMPLE!

TO READ ON, CLICK HERE & DOWNLOAD THE COMPLETE GUIDE

THE FULL EBOOK INCLUDES EASY-TO-FOLLOW STEPS AND PRACTICAL GUIDANCE FROM TIM BANDOS, A FORMER FORTUNE 100 INCIDENT RESPONSE LEADER TO HELP YOU:

1. Build your Incident Response team.
2. Implement an Incident Response plan in your organization.
3. Manage Incident Reponse with limited resources.

TO READ ON, FILL OUT OUR SHORT FORM AND DOWNLOAD THE COMPLETE GUIDE NOW >>

DIGITALGUARDIAN®