MANDIANT®
A FireEye® Company

ARE YOU READY TO RESPOND?

EVALUATE AND IMPROVE YOUR ABILITY TO RESPOND TO THE NEXT ATTACK

WHITE PAPER

FireEye®

CONTENTS

ABOUT THIS PAPER

Consultants at Mandiant, a FireEye Company, have helped evaluate and enhance the cyber security program of customers of all sizes across a range of industries around the world. This paper draws on the combined experience of our consultants over the course of hundreds of these service engagements. While we have withheld some identifying details for the privacy of our clients, the stories are real. The insights, advice and examples presented here represent more than a decade of work helping clients reduce risk and improve their security posture.

INTRODUCTION

“IN OUR CURRENT STATE OF CYBER SECURITY, SECURITY BREACHES ARE INEVITABLE. THIS IS AN IMPORTANT FACT, SO I AM INTENTIONALLY REPEATING IT. IN OUR CURRENT STATE OF CYBER SECURITY, SECURITY BREACHES ARE INEVITABLE.”[1]

With those words, FireEye Chief Executive Officer Kevin Mandia opened his testimony to the U.S. House Permanent Select Committee on Intelligence in an October 2011 hearing.

He was speaking in the wake of several high-profile data breaches that had piqued concern among law-makers. As recent headlines demonstrate, his prediction is more relevant than ever.

Given that 96% of typical defense-in-depth deployments have been breached, the question is no longer about whether you will be breached.[2] It is how you respond when it occurs, despite your best efforts to prevent it. In this era of more frequent breaches, the company with a well-designed incident response plan is better off than the company without one.

[1] U.S. House of Representatives. “Written Testimony of Kevin Mandia, Chief Executive Officer, Mandiant Corporation, Before the Permanent Select Committee on Intelligence U.S. House of Representatives Cyber Threats and Ongoing Efforts to Protect the Nation.” October 2011.

[2] FireEye. “Maginot Revisited: More Real-World Results from Real-World Tests.” January 2015.

In this era of more frequent breaches, the company with a well-designed incident response plan is better off than a company without one.

Having systems in place to prevent as many breaches as possible is only the start of a thorough defense. Today's threat landscape also requires a detailed incident response strategy to detect and respond to a breach, along with the expertise to execute it. Once you identify an attacker has infiltrated your network, you need to move quickly to minimize damage to your infrastructure, your brand and your customers.

This paper draws on our experience at Mandiant, a FireEye company, working with organizations around the world. We have helped hundreds of clients assess and evolve their ability to respond effectively to critical security incidents. We will focus on three key areas:

- Having a plan
- Having the ability to execute that plan
- Practicing the plan

Once you have a response plan, you need to make sure that you have the proper security technologies and expertise to support it. A response plan requires a full view of your IT assets, accurate detection capabilities and quick reaction time. Your team should regularly practice the response plan and keep track of multiple metrics that measure how well it is working. This insight helps you keep improving upon the plan to handle the next incident — and the next, and the next.

In many instances, we learn that companies have an incident response plan that looks good on paper but not in practice. The plan cannot just live in a manual that sits on a shelf. It needs to be a strategy that everyone agrees to, can evolve over time, is rehearsed often and can be carried out immediately when the time comes.

Why an incident response plan is essential

What was once a revolutionary thought has now become conventional wisdom: security breaches are inevitable. Security organizations need to focus more resources on building up their defenses and developing a battle plan to thwart attackers that bypass those defenses.

Think of it this way: airlines spend millions of dollars on systems to keep planes aloft. But they still install life vests and emergency escape chutes. And, they train flight crews to help passengers in the event of an emergency landing. You need to prevent as many attacks as possible but prepare for the ones that slip through your defenses.

SIX CORE CAPABILITIES FOR AN EFFECTIVE RESPONSE

Based on our experience working with clients, we have found that a well-conceived incident response plan covers six areas as shown in Figure 1. You should evaluate all of them when planning, executing and maintaining your response plan.

FIGURE 1: SIX KEY AREAS FOR EVERY RESPONSE PLAN

CAPABILITY	DESCRIPTION
GOVERNANCE	• An organizational structure that aligns with overall business organization and mission statement • Clear security policy and guidance that safeguard critical systems and information sharing between internal and external entities
COMMUNICATION	• Mechanisms and processes that promote effective information sharing between internal and external entities
VISIBILITY	• Technologies and processes that keep organizations aware of activities occurring on systems and networks • Methods by which the computer incident response team (CIRT) remains aware of the threat landscape and applies that understanding to defending critical infrastructure
INTELLIGENCE	• Cyber threat intelligence capabilities that enable a detailed understanding of the adversary's capabilities, techniques and intent • Intelligence that informs and enhances security planning, vulnerability management and incident response
RESPONSE	• Process and technologies that the CIRT uses to identify, categorize, investigate and remediate adverse security events
METRICS	• Objective measures of the efficiency of people, processes and technology using a system that can be easily tracked and automated • Focused incident response metrics that are tied to overall business and security goals and objectives, driving continuous improvement

1. Governance

Your organization's structure should align with your goals and mission statement. Employees must understand their roles and duties during an incident. You need a clear security policy to safeguard critical systems without impeding business functions. And, your response plan must comply with applicable regulations and laws.

But governance is not just about compliance. It also addresses how the staff is organized, especially when it comes to who reports to whom. We see a number of different organization charts at client companies.

In some cases, the chief information officer (CIO), who would typically manage IT systems and their security, is also the chief administration officer (CAO) — thus taking time away from IT. In other cases a chief information security officer (CISO), who reports to the CIO, focuses exclusively on security. But in still other situations, security operations center (SOC) staff report to the chief financial officer (CFO) because security was originally tasked with protecting the company's financial data. Organizational charts that may have made sense at one point of a company's development are not always ideal for good security governance.

An assessment can identify other potential conflicts in the relationship between security and the executive suite. One client in the energy sector had a director of security — not a C-level post — who reported to the CIO. The security director was often pulled in different directions and given tasks not directly related to IT security. Based on our advice, the client elevated the director of security to a CISO to focus his attention solely on IT security.

Given all these variations, detailing job duties and relationships between different personnel in the incident response plan is crucial.

If you don't communicate fully and effectively, you aren't responding effectively.

Logistical issues may come to the surface when assessing your response plan. With some clients, the SOC is located in one time zone, but the company has operations in multiple zones, even hemispheres. Should you develop a 24/7 "follow the sun" SOC model and, if so, how do you do that? In addition, how much budget do you need to build the security staff you need? We have had clients based in Detroit, Michigan that have reported trouble recruiting security professionals. We have advised them to establish their SOC in Silicon Valley, where they will find a more ample supply of skilled security workers.

2. Communication

A robust incident response plan depends on the security team sharing information with the right external entities at the right time. An external entity could be another department within the same company or third parties outside the company, including security vendors, government agencies or law enforcement. Effective communication also requires defining incidents by category or severity so that you can consult additional stakeholders as necessary if the incident escalates.

When we talk with clients about a communications plan, the proverbial "Who gets the call at 3:00 a.m.?" question often comes up. Sometimes, the answer is as simple as "Call Bob." But it gets complicated when you learn that Bob is in the mountains on vacation. Contingency plans are essential.

The response plan must lay out which stakeholders and levels of management to alert as the incident unfolds. We often see organizations discount the importance of communication because they assume it will happen on its own. It won't. If you don't communicate fully and effectively, you aren't responding effectively.

If you understand what your network is supposed to look like, then you will be better able to spot activity that doesn't belong — including an intruder.

3. Visibility

Knowing what's happening on your network is critical. You need technology and processes that provide a full view of what's going on throughout your organization to quickly detect and scope incidents. You need to remain aware of the threat landscape — and from there, be able to jump in quickly to defend your critical infrastructure.

A key measure of visibility is your ability to track activity logs for various network security appliances. The logs can alert your security team when, say, unauthorised users are on your network or an attack is underway. Visibility issues are discussed further later on in this white paper.

Assessing your visibility might reveal some major blind spots. An assessment of a pharmaceutical company client, for example, revealed that the security team could not see what was happening in the company's research and development (R&D) operations because that group had been granted exemptions from some security requirements; the group said it hindered its work. Other companies might see the situation differently, deeming R&D to be some of the company's most valuable intellectual property and protecting it as such.

Thorough visibility gives you the information you need to understand what's happening on your network. If you understand what your network is supposed to look like, then you will be better able to spot activity that doesn't belong — including an intruder.

4. Intelligence

A detailed understanding of attackers' capabilities, techniques, and intent dramatically improves the quality and speed of your response. While it's not always easy to obtain, gaining insight into what attackers are capable of doing helps you better anticipate their next move.

Some cyber threat intelligence comes from aggregating publically available information from online sources. News stories and blogs share information and advice on well-known attacks, how they unfold, and what steps you can take to protect your network from them.

In other instances, companies engage in public-private partnerships to share intelligence. An electric utility client has an agreement with a government agency: the utility shares information with the agency about what's happening on its network, and the agency lets the utility know what threats might be targeting that network. Similar info-sharing agreements exist between businesses and their network security vendors.

In some cases, these partnerships can provide more valuable intelligence than what appears on the news and in blogs. The revelations about the Heartbleed Bug generated a lot of buzz and news coverage when it was first discovered in April 2014.[3] The vulnerability in the OpenSSL cryptographic software library put a vast amount of encrypted content potentially at risk.

[3] Jose Pagliery (CNN). "Don't assume you're safe from Heartbleed." April 2014.

While OpenSSL was widely used, Heartbleed was not particularly dangerous for organizations that maintained good security habits. If your network was fully patched and up to date, Heartbleed did not affect you. Heartbleed gained a lot of traction on CNN, BBC and elsewhere, but it was not a big threat to most organizations. Even so, when C-level executives heard about Heartbleed on TV news reports, the incident did have the added benefit of increasing their awareness of cyber threats in general.

5. Incident response

The ultimate test of your security is how you respond when an actual incident occurs. You've been compromised. Now what? Your response plan must identify processes and technologies that the CIRT uses to identify, categorize, investigate and remediate security events. Before an incident occurs, you need to answer these key questions:

- Does your team have the training they need to respond effectively and efficiently to an incident?
- Does your organization have the hardware and software it needs to respond across your enterprise?

We find in many assessments that clients have only manual tools and systems to respond to a breach when automated systems can address the situation more precisely and quickly.

In one engagement, we worked with a global manufacturing company that had more than 150,000 endpoints but fewer than 10 employees managing security. The company's processes were manual and not consistent across the company. Its analysts also lacked the visibility and context necessary to identify and escalate the alerts that needed immediate attention.

Within a year, the company's incident response team was able to standardize, document, apply procedures, implement security technology and create a tiered approach that allowed it to respond more effectively to security incidents.

Surprisingly, some of the clients we deal with have an incident response plan on paper but don't refer to it when an incident occurs. They follow what they call "tribal knowledge," or institutional knowledge gained by a team through experience. Put another way, it's all the things that people know but that are not written down anywhere.

Security professionals learn from experience. For example, they can recognize that a certain event they are dealing with is a malware attack. But tribal knowledge does not help if the person with the most knowledge is unavailable or has left the company. And it does not help when a new and unknown threat appears.

6. Metrics

Metrics help organizations measure and improve how effectively and efficiently they are responding to incidents. Your metrics might include the following:

- Once you have identified a breach, how long is the attacker present in the environment before you can contain the attack?
- Once the attack has been contained, how long does it still exist in your environment before the threat is totally remediated and removed?

Comparing metrics before and after you have improved the incident response plan is key.

Assessing your response readiness allows you to subjectively analyze who is supposed to do what, how well someone can identify a threat and what technology and practices an organization should have in place.

Metrics also allow you to objectively measure how efficient your people, processes and technology are throughout a system that can be tracked and automated. Incident-response performance metrics are also valuable because they align with overall security and business goals — and are geared toward steady improvement.

In the example of the manufacturing company cited earlier, subjectively analyzing people and processes while objectively analyzing various performance metrics helped the client significantly improve its security posture. Among other things, the client was able to standardize, document, and apply security procedures. And it could tailor its response to security incidents to fit their severity using an escalation matrix. This all helped the firm to more effectively detect and respond to security incidents.

Key incident response metrics

One of the key sets of metrics that help measure clients' readiness is the time it takes to recognize that an incident is occurring and then the time it takes to contain it. The longer those times stretch, the longer the adversary has time to do harm. The shorter these times, the less vulnerable you are.

Mean time to detection

Mean time to detection measures the time between when a breach has occurred and when you discover it. This measurement includes several stages that spell out the acronym DRAIN:

- **Detect:** The time from initial entry into the network to detection. This stage gauges the effectiveness of perimeter technology such as intrusion detection systems (IDS) and firewalls.
- **Review:** Time from detection to an analyst's review of the incident. This helps determine whether your staffing level is sufficient to keep an eye on your network for threats.

YOU CAN'T DEFEND WHAT YOU CAN'T SEE

Why visibility is key to an effective response plan

The cyber security industry is rife with tools that generate alerts based on programmed rules and heuristic analysis. It's no wonder that the typical SOC receives more than 500,000 alerts per day.[4] The downside is sorting out which of these alerts actually matter.

Visibility is one of the key capabilities to emphasize when assessing your readiness, because no security in the world will matter if you cannot tell the difference between alerts to which you should respond and alerts to which you must respond. Often, breaches happen because people overlook critical alerts amid all the noise.

To enhance the security visibility of a network, prioritizing different alerts is critical. Equally important is understanding what combination of alerts adds up to a critical situation.

Security monitoring occurs on a network through an analysis of appliance logs. Feeds from these appliances flow through an aggregator that then helps create rules to issue alerts. Warnings from appliance A mean one thing. Simultaneous warnings from appliances A, B and C mean something much more serious, warranting a higher alert. If you also get an alert from appliance F, it's "Battle stations, everyone!"

In network security parlance, alerts that sound simultaneously from multiple points on the network can be a strong sign of an advanced persistent threat (APT).

Visual cues are also important for prioritizing alerts. On your system dashboard, a green light may indicate a minor alert, while a red light — maybe flashing and beeping as well — indicates a critical one.

Mandiant has identified 13 different types of logs that generate alerts. Besides the usual antivirus, firewall and intrusion detection system (IDS) warnings, logs also identify anomalies generated by alerts in Citrix appliances, Windows or Linux environments, virtual private networks (VPN), open wireless architecture (OWA) and web-facing servers (just to name a few).

Having so many appliances that can trigger alarms makes responding to the important ones difficult. The alerts that really matter get lost amid all the noise. And many alerts are false alarms, obscuring the threat environment even further.

To respond to the most critical alerts immediately, your system needs to provide a complete, clear view of your threat situation — one that you can act on.

A first step should be to reduce the volume of trivial and false alerts by dynamically analysing them in real time using virtual-machine technology. You should also deploy technology that groups together alerts that may stem from the same attack — such as an APT, for example — so the security team has a more holistic view of the situation.

An important complement to your visibility capability is intelligence to identify widely known threats and threat actors. You can compare their signatures and behavior to what you are seeing on your network.

Surprisingly, some alert systems fail to provide information to the security team about how to respond to an alert. The staff has to figure out on their own what specific systems are under attack, what information is at risk, and what steps to take to stop the attack and restore order.

Having improved visibility into the threat environment helps make your incident response program more effective.

[4] FireEye customer data.

- **Analyze:** The time taken to analyze the incident. As you dig further into the threat, you need to determine if the organization has the right expertise and tools to know what to do if the event escalates.
- **Identify:** The time taken to identify affected assets — a group of servers, for example — their location and their owner. The owner could be a specific department within your organization or an outside vendor. This step helps measure the effectiveness of the organization's asset inventory management.
- **Notify:** The process of alerting appropriate contacts. This step measures the effectiveness of a contact database and a communication plan that determines, say, who gets that 3:00 a.m. phone call.

Mean time to resolution

Mean time to resolution is the time between an organization discovering a breach and resolving it. This measurement includes the following key elements, which form the acronym CVR:

- **Collect:** Time to collect live response data from the network to manage the breach. This step determines if you are deploying the right tools to assist in collection.
- **Validate:** Time to confirm the extent of the intrusion based on that collected data. This helps determine if the right skills are in place at each level of your organization.
- **React:** Time to contain and remove the threat. This measures whether the remediation is applied correctly, consistently and as quickly as possible.

A response readiness assessment typically reveals areas that are ripe for improvement, and it can help organizations prioritize what changes to make. If they cannot completely eliminate the risk of damage from a breach, they can at least reduce it to a tolerable level.

The DRAIN/CVR process serves many purposes for a company assessing its response readiness. It helps measure how its response capability has improved over time, particularly after it has improved its systems after a breach. Security leaders can also measure their readiness over time as their company grows and adds more endpoints and more complexity to its IT infrastructure.

Clients also tell us they want to compare their readiness to that of industry peers. This kind of comparison might have some value, but we caution clients that it does not directly indicate how prepared they are to respond to threats.

Security leaders can measure their readiness over time as their company grows and adds more endpoints and more complexity to its IT infrastructure.

HOW DO YOU RANK FOR READINESS?

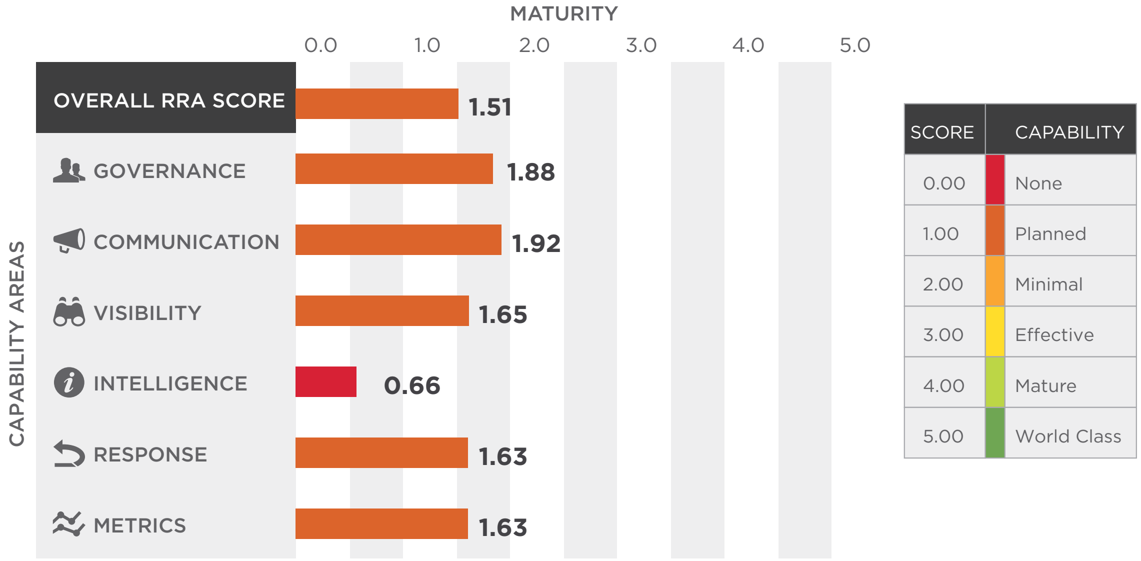
Mandiant ranks each of the six plan capabilities on a scale of 0–5 as follows:

- **0.00 No capability:** There is no recognizable process. The organization does not see a problem and there is no communication on the issue. No one ever gets a zero ranking because clients always have some kind of security technology. But this score serves as a baseline.
- **1.00 Planned capability:** The company has made a commitment to implement new security technology and procedures, but the project has not yet been completed.
- **2.00 Minimal capability:** The company has some security in place, but it is bare bones and unlikely to protect against things such as APT actors.
- **3.00 Effective capability:** The company has security in place that meets industry standards.
- **4.00 Mature capability:** The company has security in place that exceeds industry standards.
- **5.00 World class:** The company has security that is the envy of the National Security Agency. Your security chief is a frequent guest speaker at industry events. Others aspire to this standard. Few companies get a five — it would be prohibitively expensive for most.

We present the results of the rankings to the client in a bar graph, as shown in Figure 2. As the graph indicates, a client can achieve a high ranking in some areas and a lower ranking in others. This helps leaders determine where they are strong and where they need to improve their security.

The client assessed in Figure 2 ranked highest on its communications capability, but ranked very low on its ability to gather intelligence on network threats.

FIGURE 2: SAMPLE RESPONSE READINESS ASSESSMENT SCORE



OUR APPROACH TO ASSESSING YOUR READINESS

Mandiant can help you gauge your overall security posture, including the six core capabilities outlined earlier. Our Response Readiness Assessment also measures how effectively your team detects and contains an incident. And it outlines how your SOC and CIRT are organised.

The Response Readiness Assessment covers the areas detailed below. It follows the three-step process shown in Figure 3.

FIGURE 3: MANDIANT'S RESPONSE READINESS ASSESSMENT

STEP 1	STEP 2	STEP 3
Assess your ability to detect, respond to and contain threats Mandiant experts collect and review your security operations, threat intelligence and incident response program documentation to compare the baseline of your current practices against industry best practices.	**Put your processes to the test with tabletop exercises** We work with you to customise a scenario that simulates an incident. Common scenarios include system compromise, internal leak of personally identifiable information (PII), or an internal investigation of inappropriate use and threatening email. During the response, we assist and evaluate the effort from initial detection to resolution.	**Mandiant recommendations and roadmap** We provide you with a final report and presentation that blends our review of your procedures, your staff's insights, and our observations during the exercise. We focus on benchmarking your program against applicable legal or regulatory requirements and industry best practices, highlighting your program's strengths and opportunities for improvement.

Assess capabilities

Our consultants provide an independent assessment of your current security monitoring and response capabilities, leveraging intelligence from our expert incident responders who work with compromised organizations around the world on a daily basis. Because we are usually brought in after a breach, we know how their response plan failed. That vantage point gives us a unique insight into what works.

One client signed us up in the midst of an already-in-progress five-year security overhaul. It wanted to make sure it didn't go through the whole five years and fail to maximize security or create a response plan. While we were happy to help, it is usually best for Mandiant to come in before an organization has gone too far down the path with its plan.

Review best practices

We explain incident response best practices and ways to structure your SOC workflow. We also help you integrate your security information and event management (SIEM) tools with your incident response practices. We bring to the process our history as an incident response and intelligence company. Our customer base includes multiple Fortune 500 companies, many of which are breach victims already. That experience informs our advice for even more clients.

Review latest threats

We brief clients on the latest threats we have seen and how to thwart them. Before each onsite visit with a client, our consultants meet with FireEye intelligence teams to obtain the latest information on emerging threats. In many cases, our consultants can speak with authority about the different threat actors that may be targeting companies in your specific industry.

Practice responding

We help you practice incident response with specially designed drills based on actual incidents that we have seen in the wild. We call the drills a "tabletop exercise," where we present an attack scenario to the participants. Along the way, we add various "injects" to the drill, as if they were plot twists in a movie thriller.

In one scene, an employee inadvertently opens a phishing email; in the next, the malware carried in the fake email exposes a CEO's real email revealing a proposed merger. The question after each inject is "How do you respond?"

The exercise is especially revealing when their response in the drill differs from the company's documented policies and procedures, and their behaviour in a similar incident that they actually experienced.

Recommend project roadmap

A project roadmap lays out what improvements are needed, based on what will generate the greatest return and have the biggest impact on your security posture. Mandiant consultants offer short, medium and long-term capital and operating budget recommendations based on the client's priorities and finances.

CONCLUSION

As Kevin Mandia said during his 2011 House testimony, acknowledging that breaches are inevitable is not the same as giving up the fight. "While this [reality] sounds defeatist," he testified, "we are not defeated."

A Mandiant Response Readiness Assessment can help determine how well equipped your organization is to prevent, detect, analyze and respond to the inevitable breach.

The ultimate goal: adopt a response readiness architecture that prevents many breaches outright, detects more advanced attacks as soon as possible, analyzes the threat to quickly understand the scope, and responds quickly to avoid lasting harm and get back to business.

As with the airliner analogy about life vests, escape chutes and flight crew training, you hope you never have to use them — but if you do, they need to work.

To learn more about FireEye and Mandiant intelligence-led consulting services, visit: **www.FireEye.com**

FireEye, Inc.
1440 McCarthy Blvd. Milpitas, CA 95035
408.321.6300 / 877.FIREEYE (347.3393) / info@FireEye.com

www.FireEye.com