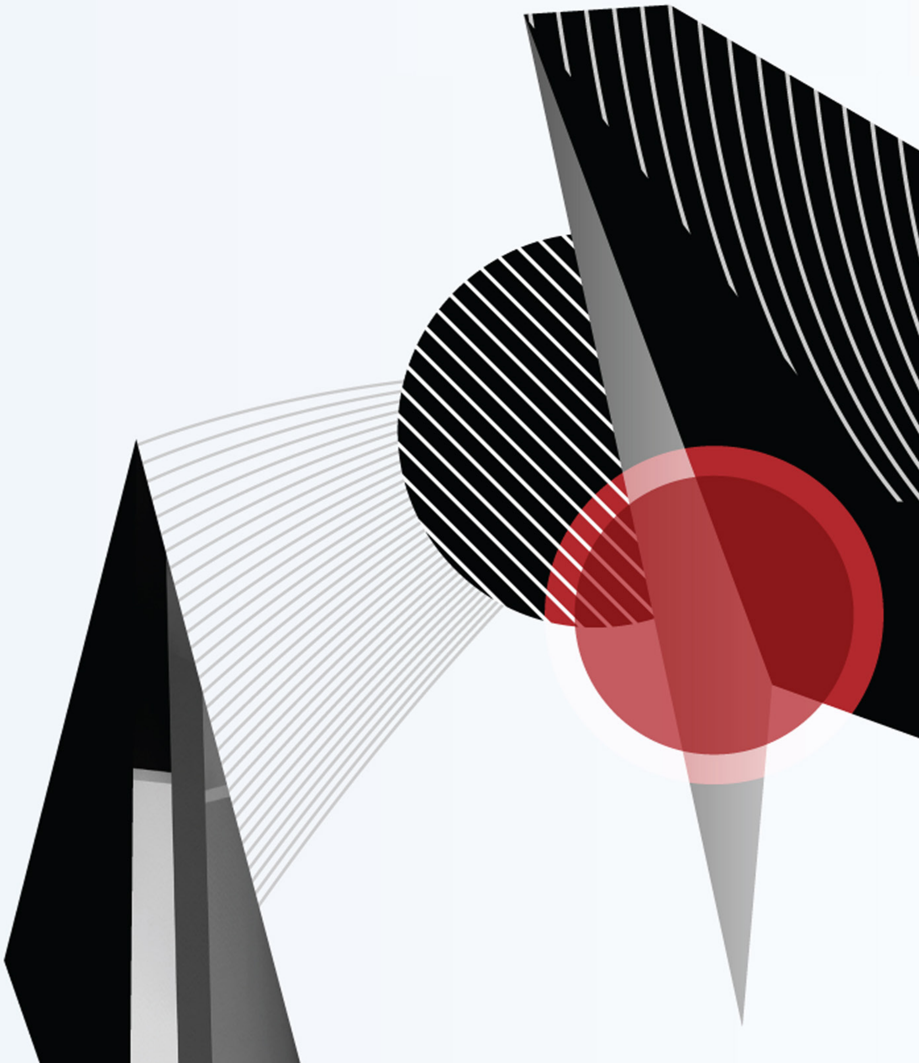
WHITE PAPER

How to Prepare for a Cyber Attack

Six core capabilities model



"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 a previous 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.

The question is no longer "will you be breached," but "how will you respond when you are breached," despite your best efforts at prevention. The organization with a well-designed incident response plan has a much greater advantage than the organization without one.

Having detection technology in place is only the start of a thorough defense.

Today's threat landscape also requires a detailed incident response strategy to detect, respond to, and contain a breach, along with staff expertise to implement that strategy. Once it's determined that an attacker has infiltrated your network, you must move quickly to minimize damage to your organization's infrastructure, brand and customer base.

This paper draws on the worldwide incident response (IR) experience of Mandiant, a FireEye company, to explore the three phases of preparing for a cyber attack:

- Developing an effective IR plan
- Adopting the proper capabilities to execute that IR plan
- Practicing the IR plan

Once you have a response plan in place, you need 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 various metrics that measure how well it is or isn't working. This helps you continually improve the plan to properly handle subsequent incidents.

Many companies have an incident response plan that may look good on paper but execution has not been tested. Key stakeholders must agree on the strategy, evolve it over time, and be able to implement it confidently during an incident.

[1] U.S. House of Representatives (October 2011). "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."

The Importance of an Incident Response Plan

Security teams need to focus more resources on building up their defenses and developing a battle plan to stop attackers that outmaneuver those defenses.

For example, aircraft companies spend millions of dollars on mechanical and avionics systems to maintain and improve aircraft safety. But they still enable the installation of life vests and emergency escape chutes. Airlines train flight crews on emergency procedures. And passengers receive training before every flight. Your security program should prevent as many attacks as possible, but you should also prepare for attacks that slip through your defenses.

Six Core Capabilities for Effective Response

Mandiant consultants have found that an effective incident response plan addresses six core areas (Table 1). Evaluate all of them when planning, executing and maintaining your incident response plan.

Table 1. Six key areas of an effective response plan.

Capability	Description
Governance	• An organizational structure that aligns with overall business objectives and mission statement • Clear security policy that safeguards 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 stakeholders aware of activities occurring on systems and networks • Methods by which the cyber 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	• CIRT processes and technologies used to identify, categorize, investigate and remediate incidents
Metrics	• Objective measures of people, processes and technology that can be easily tracked and collected automatically • Focused IR metrics tied to overall business goals and security objectives, driving continuous improvement

Governance

Governance is more than compliance with applicable regulations and laws.

Governance includes ensuring that the security team's structure aligns with an organization's overall goals and mission statement, supported by employees who understand their specific roles during an incident.

Roles and responsibilities are reinforced by leadership, making it crucial to establish a suitable reporting structure across the team.

In some cases, the chief information officer (CIO), who typically manages 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) focuses exclusively on security. Sometimes 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 sound security governance.

A security program assessment can identify potential conflicts due to reporting relationships between a security team and the executive suite. If a security director reports to the CIO, security-focused initiatives may not be prioritized or adequately resourced.

Given these variations, it is crucial to detail job duties and relationships of personnel across the entire incident response plan.

Logistical issues may come to the surface when assessing your response plan. With some clients, the SOC is located in one time zone, though the company has operations in multiple zones, even hemispheres. In this case, the security team should develop a suitable 24/7 "follow the sun" model.

Communication

A robust incident response plan depends on quickly sharing information with the appropriate internal and external parties. This could be another department within the same organization or third parties outside the company, including security vendors, government agencies and law enforcement.

Effective communication requires defining incidents by category or severity. This expedites stakeholder notification if an incident escalates. The response plan must define which stakeholders and levels of management to alert as an incident unfolds. Contingency plans are essential when critical security staff are unavailable due to illness or vacation.

Without full and effective communication, you cannot respond effectively. And organizations should not assume proper communication will occur naturally.

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

Visibility

It is vital to know what is happening on your network every day. Technology and processes should provide visibility throughout your organization to quickly detect and scope incidents to scale. Awareness of your threat landscape enables you to quickly defend your organization's critical infrastructure.

One effective way to measure visibility is through your ability to track activity logs for various network security appliances. Logs alert your security team when, unauthorized users are in your network or worst case, an attack is underway.

Assessing your visibility can reveal blind spots. For example, if a group in your organization is granted exemptions from certain security requirements to speed up network processes, their networks may not be fully visible to the security team.

Understanding what your network is supposed to look like, better equips you to spot activity that doesn't belong — including an intruder.

> Understanding what your network is supposed to look like, better equips you to spot activity that doesn't belong — including an intruder.

Intelligence

A detailed understanding of attacker tactics, techniques, and procedures (TTPs) dramatically improves the quality and speed of your response. While this information is not always easy to obtain, gaining insight into attacker TTPs helps you better anticipate their next move.

Some cyber threat intelligence comes from aggregating publicly available information from online sources.

News stories and blogs share information on well-known attacks, how they unfold and what steps you can take to protect your network from them. However, a security team should never rely on publicly available information alone.

In other instances, companies engage in public-private partnerships to share intelligence. For example, a utility company may have an agreement with a government agency: the utility company might share network activity information with the agency, and the agency might inform the utility company of threats that might be targeting their network. Similar information-sharing agreements exist between businesses and their network security vendors.

These partnerships can provide more valuable intelligence. Revelations about the Heartbleed Bug generated a lot of news coverage when it was first discovered in April 2014.[2] The vulnerability in the OpenSSL cryptographic software library put a vast amount of encrypted content potentially at risk.

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 major news outlets, but it was not a major threat to most organizations. Regardless, when C-level executives heard about Heartbleed from the news, it increased their overall awareness of cyber threats.

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

Response

The ultimate test of your security posture is how you respond when an actual incident occurs. Your response plan must identify the processes and technologies that your cyber incident response team (CIRT) uses to identify, categorize, investigate and remediate security events. Before an incident occurs, you need to answer these key questions:

- Did your team receive suitable training to respond effectively and efficiently to an incident?
- Does your organization have the right hardware and software to respond across your enterprise?

If you employ a smaller team that uses manual tools and systems to respond, consider adopting automated systems that can address suspect events more precisely and quickly.

A security plan on paper is only part of the solution. Relying on institutional knowledge rather than the written plan can result in poor security behavior, especially if key personnel are absent or never-before-seen threats appear.

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. The typical SOC receives more than 500,000 alerts per day.[4] Organizations need to spend valuable time sorting out which alerts actually matter.

Visibility is a critical criteria for assessing your readiness. Effective and efficient security relies on being able to tell the difference between alerts to which you should respond and alerts to which you must respond. Breaches often occur because people overlook critical alerts amid all the noise.

To enhance security visibility, you must prioritize alerts and recognize which combination of alerts can lead to a critical situation.

Network security monitoring occurs 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, you should know that you must mobilize your entire security team immediately.

In network security parlance, alerts that sound simultaneously from multiple points on the network can be a strong sign of a targeted attack.

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

Mandiant experts have 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 on vendor-specific network appliances, as well as in Windows or Linux environments, virtual private networks (VPN), open wireless architecture (OWA) and web-facing servers (just to name a few). Having many sources of alerts, including many false alerts, can severely obscure the threat environment.

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.

First, reduce the volume of trivial and false alerts by dynamically analyzing them in real time using virtual- machine technology. Deploy technology that groups alerts that may stem from the same attack — such as an APT attack — so the security team can view the situation holistically.

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.

Some alert systems fail to provide response information to the security team. The staff must work to discover what specific systems are under attack, what information is at risk and what steps to take to stop the attack and restore order.

Improved visibility into the threat environment can help make your incident response program more effective.

[4] Unpublished FireEye customer data.

Metrics

Metrics help organizations measure and improve how effectively and efficiently they respond to incidents. Metrics could include the following:

- After you identify a breach, how long does it take your team to contain the attack?
- After the attack has been contained, how long does it take to fully remediate and remove the threat from your environment?

You can evaluate progress by comparing metrics before and after you improve the incident response plan.

Assessing your response readiness allows you to subjectively analyze which responsibilities are assigned to which personnel, how well someone can identify a threat and what technology and practices should be in place.

Metrics also 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.

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

Key Response Metrics

One of the most important sets of metrics that helps measure readiness is the time it takes to recognize an incident is occurring and the time it takes to contain it. The longer those times stretch, the more time the adversary has to do harm.

Mean Time to Detection

Mean time to detection (dwell time) measures the time between when a breach has occurred and when it is discovered. This measurement includes several stages:

- **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 a close eye on your network for threats.
- **Analyze:** The time taken to analyze the incident. As you explore the threat further, you must determine if the proper tools and expertise are in place to take action if the incident 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 who might get a 3:00 a.m. phone call.

Mean Time to Resolution

Mean time to resolution measures the time between when an organization discovers a breach and when it resolves the breach. This measurement includes the following elements:

- **Collect:** Time to collect live response data from the network to manage the breach. This step determines if you are deploying the correct collection tools.
- **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 reveals areas of opportunity for improvement, and can help organizations prioritize what changes to make. If an organization cannot completely eliminate damage from a breach, they can at least reduce the risk to a tolerable level.

Collectively, both detection and resolution processes serve many purposes for a company assessing its response readiness. They help measure how its response capability has improved, particularly after a recent breach. Security leaders can also measure readiness over time as their organization grows and adds more endpoints and complexity to its IT infrastructure.

Some organizations may want to compare their readiness to that of industry peers. This kind of comparison can have some value, but it does not directly indicate how well-prepared an organization is to respond to threats.

Determine Your Readiness Rank

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

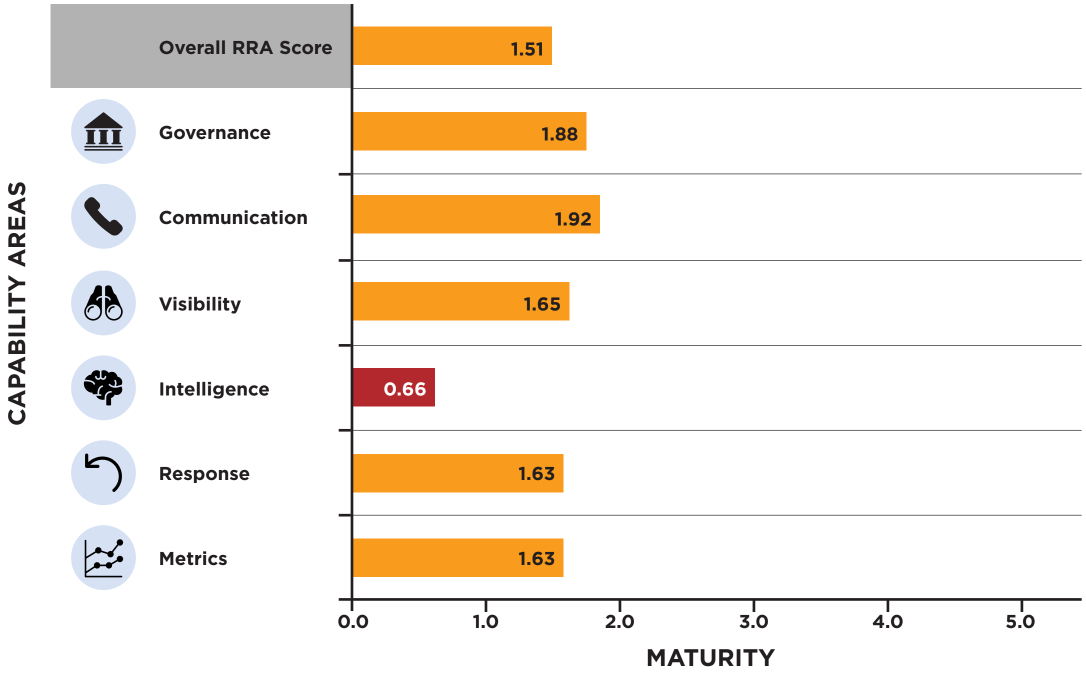
- **0.00 No capability:** There is no recognizable process. The organization does not see a problem and there is no communication on the issue. A zero ranking is not possible; organizations always have some kind of security technology. But this score serves as a baseline.
- **1.00 Planned capability:** The organization has made a commitment to implement new security technology and procedures, but the project has not yet been completed.
- **2.00 Minimal capability:** The organization has some security in place, but it is bare bones and unlikely to protect against things such as advanced persistent threat (APT) actors.
- **3.00 Effective capability:** The organization has security in place that meets industry standards.
- **4.00 Mature capability:** The organization has security in place that exceeds industry standards.
- **5.00 World class:** The organization 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.

Ranking results are presented to clients in a bar graph (Fig. 1). A client can achieve a high ranking in some areas and a lower ranking in others. This helps security leaders determine where they have strong capabilities and where they need to improve.

The hypothetical client assessed in Figure 1 ranked highest on its communications capability, but ranked very low on its ability to gather network threat intelligence.

Figure 1. Sample Response Readiness Assessment score.



Score		Capability
0.00	🟥	None
1.00	🟥	Planned
2.00	🟧	Minimal
3.00	🟨	Effective
4.00	🟩	Mature
5.00	🟩	World Class

The Mandiant Approach

Mandiant experts can help gauge your organization's overall security posture, as well as its facility with the six core capabilities. The Mandiant Response Readiness Assessment also measures how effectively your team detects and contains an incident, and evaluates how your SOC and CIRT are organized.

The Response Readiness Assessment follows the three-step process shown in Table 2.

Table 2. Mandiant Response Readiness Assessment.

Step 1	Step 2	Step 3
Assess your ability to detect, respond to and contain threats Mandiant consultants review your SOC and IR documentation, and compare your current processes against industry best practices to establish your baseline performance. They also conduct detailed staff interviews to better understand SOC and IR processes that are unique to your organization.	**Test your processes with tabletop exercises** Incident scenarios (such as system compromise, unauthorized access of personally identifiable information (PII), policy violations, inappropriate emails) are simulated to evaluate your organization's response processes from incident detection to closure.	**Adopt recommendations and custom roadmap** The observations identified during documentation review, staff interviews, and the tabletop exercise will be used to develop the final report and presentation. Your organization will be benchmarked against legal and regulatory requirements, and industry best practices. The RRA will highlight your organization's SOC and IR strength's, and identify improvement opportunities.

Assess capabilities

Mandiant 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 the consultants are typically brought in after a breach, they can clearly identify shortcomings of existing response plans. That vantage point provides unique insights into what actually works.

Review best practices

Mandiant consultants provide incident response best practices and ways to structure your SOC workflow. They can also help integrate your security information and event management (SIEM) tools with your incident response practices.

Review latest threats

Mandiant experts brief clients on the latest threat groups and how to outmaneuver them. Before each onsite visit with a client, Mandiant consultants obtain the latest information on local and global emerging threats. Our consultants can speak with authority leaders about the different threat actors that may be targeting companies in your specific industry.

Practice responding

Mandiant consultants can help you practice incident response with specially designed drills based on real-world incidents. These tabletop exercises present an attack scenario to participants with various "injects," similar to 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 actual email revealing a proposed merger. The question after each inject is "How do you respond?"

The simulated exercise is especially revealing when responses in the drill differ from an organization's documented policies and procedures, and are compared to actual behaviors in previous, similar incidents.

Recommend project roadmap

A project roadmap presents necessary improvements based on what will generate the greatest return and have the biggest impact on your organization's security posture. Mandiant consultants offer short, medium and long-term investment recommendations based on your organization's risk tolerance, budget and overall business objectives.

Conclusion

As Kevin Mandia said, 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 is for organizations to 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 normalize business operations.

The hope is to never have to use your incident response plan — but if and when you do use it, it needs to work.

To learn more about Mandiant response readiness services, visit: **www.FireEye.com/services.html**

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

About FireEye, Inc.

FireEye is the intelligence-led security company. Working as a seamless, scalable extension of customer security operations, FireEye offers a single platform that blends innovative security technologies, nation-state grade threat intelligence and world-renowned Mandiant® consulting. With this approach, FireEye eliminates the complexity and burden of cyber security for organizations struggling to prepare for, prevent and respond to cyber attacks. FireEye has over 6,600 customers across 67 countries, including more than 45 percent of the Forbes Global 2000.

FireEye®