MANDIANT®
A FireEye® Company

HOW SECURE DO YOU WANT TO BE?

EVALUATING AND EVOLVING YOUR SECURITY PROGRAM

WHITE PAPER

FireEye®

CONTENTS

ABOUT THIS PAPER

Consultants at Mandiant have helped evaluate and enhance the cyber security programs 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.

ALL ALONG, YOU THOUGHT YOU WERE SECURE.

THEN YOU GET THAT CALL FROM LAW ENFORCEMENT THAT YOUR ORGANIZATION HAS BEEN COMPROMISED. NOW YOU HAVE TO PONDER SECURITY ALL OVER AGAIN.

This imagined scenario is more common than it might seem. In 2015, there were 38 percent more security incidents detected than in 2014.[1] And from the 781 publicized breaches in 2015, over 169 million personal records were exposed.[2] And in 53% of incident response engagements in 2015 by Mandiant compromised organizations learned of the breach from an outside entity.[3]

1 PwC. "The Global State of Information Security Survey 2016." October 2015.
2 Identity Theft Resource Center (ITRC). "Data Breach Reports." December 2015.
3 FireEye. M-Trends, February 2016.

With all of the competing priorities for budget and resources, every security leader must ask that all-important question: "How secure do we want to be?

"When companies are notified that they have been victimized by malicious cyber actors, it should be a wake-up call," White House cyber security coordinator Michael Daniel told The Washington Post in a 2014 statement. "U.S. businesses must improve their cyber security."[4]

That can be a daunting task, given the wide range of risks, solutions, budget limitations and so many unknowns. With all of the competing priorities for budget and resources, every security leader must ask that all-important question: "How secure do we want to be?"

It's the same question we ask when we first meet with a board in our security engagements, usually after a breach.

"The best!" someone invariably answers, fist pounding on the table. "We want to be the best in the world!"

But as we explain to clients what "the best" looks like — and the level of investment in technology and people it takes to deliver it — they quickly start to ask what the second- or third-best level of security looks like.

Ultimately, the scope of your security program depends on what level of risk you can stomach. As boards consider that question, the proliferation of high-profile attacks is making that calculation much more tangible.

We are increasingly seeing directors get out in front of the issue. When they ask us where they should start, the first step we advise is to make sure that their IT security and operations managers are on the same page when it comes to the level of risk they are comfortable with. With that in hand, it is then possible to evaluate your security program and identify what changes, if any, are required to evolve your security to address those risks.

[4] Ellen Nakashima (The Washington Post). "U.S. notified 3,000 companies in 2013 about cyberattacks." March 2014.

STEP ONE: HOW SECURE IS SECURE?

As you make your own judgment about how secure you want to be, keep in mind that your security program should match the sophistication of the threat your organization faces. Consider the unique traits of your industry and other factors.

Figure 1 shows the levels of capability we typically encounter in the field.

Your security posture probably falls into one of these categories:

- **Tools-based.** You have commonly used security tools such as antivirus (AV) software, intrusion detection system (IDS), firewalls and a person to manage them. This approach can protect you from conventional threats online.
- **Integrated framework.** You comply with commonly adopted standards such as Payment Card Industry (PCI), the Health Insurance Portability and Accountability Act (HIPAA) and rules from agencies such as the Securities and Exchange Commission (SEC) and the National Institute of Standards and Technology (NIST). You track compliance on a spreadsheet, and share your data with auditors. This approach can protect you from certain forms of cyber crime. But compliant does not equal secure. Companies technically in compliance can still get breached.
- **Dynamic defense.** You invest over and above what is required to be compliant. Your security is at least as good as others in your industry, and perhaps a little bit better. You actively hunt for cyber threats. If you lack visibility into parts of your network, you obtain it. You use threat intelligence to prioritize those threats. In short, if you were breached, you could still show outside parties — auditors, shareholders and the public — that you were as good as everyone else in your industry and that you took reasonable steps to protect yourself.
- **Resilient.** Your security is so strong that your own people don't know how to break into your network. You have detection in depth of exploits, malware, fraudulent credentials and data leakage. You generate your own intelligence and don't rely on others to tell you when you have an incident. This is the highest level of security you would need to protect yourself from nation-state attacks on your network.

FIGURE 1: Organizations need to evaluate the risks they face and invest appropriately. While being compliant is sufficient for some organizations, others want to ensure that they can withstand third-party inspection if they experience a serious security incident.

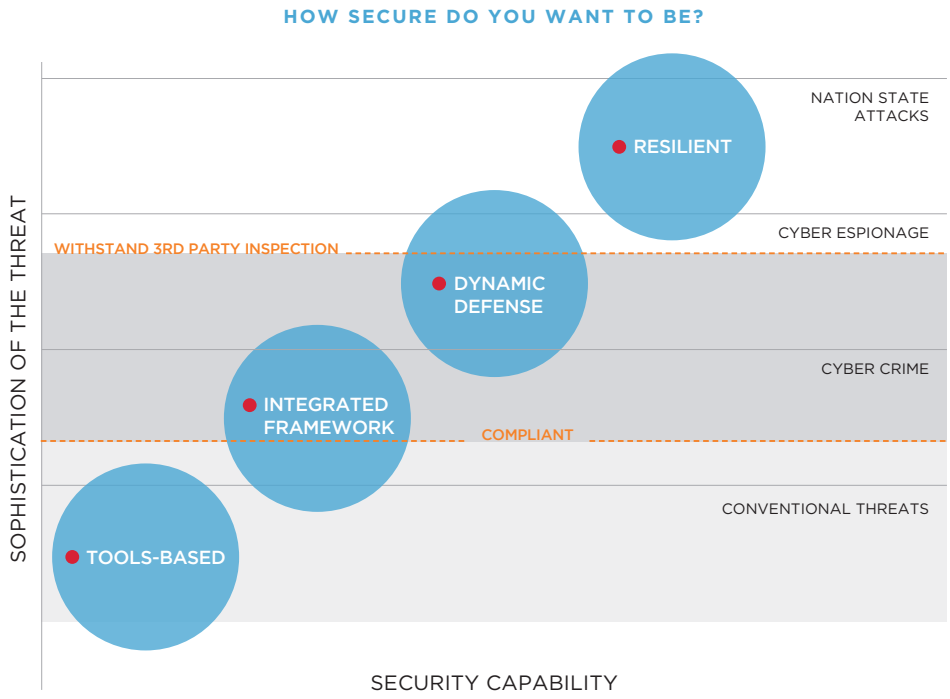
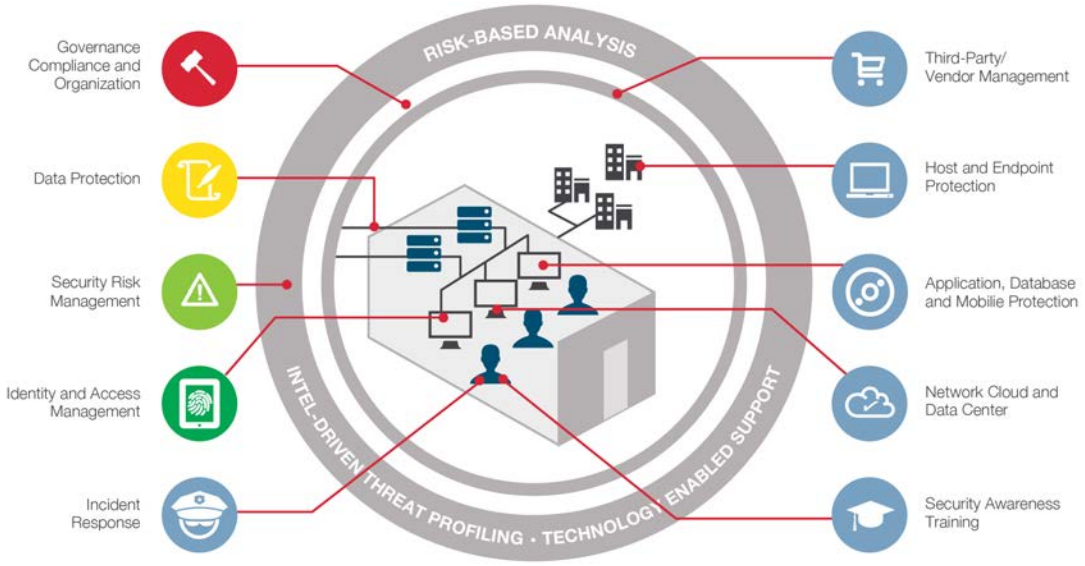


FIGURE 2: TEN AREAS TO EVALUATE



Once you know what risk you are comfortable with and the level of security you want to achieve, it is time to assess your current security program. A thorough assessment should address the 10 areas shown in Figure 2. Together, these define your security profile and can identify weak spots that need to be strengthened.

In the following 10 steps, we share real-world examples of what some of our clients discovered as they went through this process:

Identify your business objectives, governance and policy

You must first ask yourself how security relates to your core business objectives. For example, if you want customers to buy products on your website, what security do you need to keep that site up?

Another governance consideration is how your business is bound by industry standards such as PCI and HIPAA. Identifying the company's business objectives can sometimes reveal a gap between business concerns and security concerns. Security is often an afterthought at organizations whose primary focus is on marketing, sales and earnings.

A defense contractor emphasizes security because the U.S. Department of Defense insists on it. Some pharmaceutical clients might not feel the same urgency. They should. Their drug formulas are important intellectual property. If someone steals, say, the formula for a new drug, dishonest rivals could use it to develop their own products, materially harming the victim's earnings for years.

Identifying the company's business objectives can sometimes reveal a gap between business concerns and security concerns. Security is often an afterthought at organizations whose primary focus is on marketing, sales and earnings.

Protect your data

Most attackers' ultimate objective is to steal your data. So carefully assessing where your most sensitive data resides and how you are protecting it is critical. You should determine what data encryption and protection technology you use now and whether it is adequate.

Understand that data needs to be protected at rest, in use and when it is in motion across the network. You also want to classify data based on its sensitivity. Customers' personal information, for example, is more sensitive than the menu in the company cafeteria.

Data protection needs to vary by industry sector. In the oil and gas sector, for instance, we have seen clients focus on protecting proprietary seismic data, drilling techniques and extraction methods. The team assessing your security must have industry-specific knowledge about how sensitive data is stored.

Data protection policies for such things as PCI data and personally identifiable information (PII) are straightforward. But protecting intellectual property (IP) can be tougher. That's because IP can be hard to define; you need to think about it from an attacker's perspective. It can include patents, new product details and designs, software code or algorithms.

We routinely work with clients to do an inventory of their IP based on what we have seen attackers steal. In one case, a company that manufactures telecommunications equipment had the specifications for a new product stolen from their network by a cyber criminal in China before the company had a chance to patent it. Lesson learned: you have to protect IP, especially when it's still being developed.

Assess your security risk

As you begin your security assessment, acknowledging the pervasiveness of cyber crime is crucial. Your assessment must identify, address and manage the specific security risks in your environment and the tools available to reduce those risks.

Learning how others in your industry assess their risk is also important. A widely publicized breach of a major retailer might prompt executives at other retailers to ask "Could that happen to us?"

But comparing your security to that of a competitor only goes so far. For example, two companies may be fierce rivals in the beverage market. However, those companies may also be conglomerates. One may own a food company and restaurant chains. The other may own a movie studio.

In other words, rivalry in one market does not imply identical security needs. The most important thing is to make sure that your security posture matches your business, threats and risks.

The issues can vary based on the type of technology that has been implemented. For example, during an assessment of a financial services firm we found that it had poorly implemented multiple security information and event management (SIEM) instances. It also had trouble monitoring security across the enterprise and inadequate logging policies.

Your assessment should extend to human resource policies as well. For example, background checks and interviews of job applicants could reveal security risks. At one client, we found a cyber criminal had tried to get a job at a company specifically to compromise it from the inside.

A security assessment helps confirm the old adage: You're only as strong as your weakest link.

Manage access

One of the security risks we often uncover is lax restrictions on who has access to data. The looser the restrictions, the more data left open to people who have no legitimate reason to see it.

You must decide who gets access to what systems, files or applications relative to their job duties. A sales person, for instance, should not have access to human resource files. That might seem obvious. But access management can be a gray area where information is shared between business units, stored in shared folders on the network and discussed in multiple e-mails.

Also, you must review and revise access management often. You may open floors 14 and 15 to a carpet cleaning crew on certain days. But when the crew has finished the 14th floor and moved up to the 15th, you need to revoke its access to the 14th floor. And when employees move from one department to another, their access privileges should adjust accordingly.

The sophistication of access management should evolve, too. It may not be enough to just enter a password to gain access to secured data. Increasingly, we advise clients to use two-factor authentication in case passwords are compromised.

However, just improving access technology is not enough. You must actively watch for suspicious activity. Say you have an employee in California. If that person logged in from the usual location but logged in again from Russia an hour later, that's a red flag that his or her credentials have been compromised. Another red flag: an employee that usually reviews accounting databases suddenly begins transferring customer credit card data; that's a likely breach.

Review organization and resources

To provide the best security you can, review your organizational chart to make sure all of your bases are covered. You should also give your security department the budget it needs. Establish specific roles and responsibilities for employees around security, again based on their title. Your security assessment should also look at whether you have enough people on your security staff to protect the company, given its size and risk profile.

What we have found with a number of clients is that security responsibilities have grown in a piecemeal fashion over the years without regard to whether that is still an appropriate security function now. In some cases, e-discovery is a function within security because people with security know-how helped set it up. In fact, e-discovery is more a function of the legal or financial departments. If the responsibility falls to security, that leaves less money for security to protect the enterprise.

Another function that has fallen to security to manage is compliance. We have had client situations where security is tasked with making sure that employees don't watch pirated movies or download other prohibited content from sites like BitTorrent. That's a sensible policy, but security should be able to prioritize BitTorrent as a lower-level issue than an advanced persistent threat (APT) actor.

So in terms of proper allocation of resources, it's not just about how many security people you employ. It's not just a resource problem, but a process problem as well.

Another resource issue relates to how security supports the business model. The chief information security officer (CISO) at an oil and gas company told us that she wants the business side to understand the value of investing in security. That's because preventing a breach avoids the cost of remediation efforts, such as reimaging compromised servers, or the opportunity cost of lost sales when your site is down.

But some companies we encountered simply add to the job duties of existing employees without first determining whether they have the right skills to take on those tasks. If your organization wants to assure the public — including customers, partners and shareholders — that it values security, take a thoughtful approach to building and organizing your security team.

Establish an incident response plan

When attackers bypass your defenses, the ensuing breach is the ultimate test of your security program. Creating a detailed response plan ahead of time is essential. This plan should include a chain of command that delineates who does what. And it should detail how to determine whether an incident has escalated to the point where the security team needs to summon C-level executives or an outside security vendor.

In many cases, our clients may have a great incident response program on paper, but it fails in practice. While they use an academic thought process to create the plan, they may have just a handful of people who truly understand and can implement it in real life.

Plans can also fail if they are designed from a cookie-cutter template and not tailored to your particular situation. The key here is to "operationalize" the plan. Make sure that everyone who'll be involved has practiced enough to know what they're supposed to do.

Our assessment of one utility company's response plan prompted it to establish a global response program. The utility also set up a program to manage vulnerabilities and signed up for remote and on-site managed services to improve detection and response.

Incidents can also reveal weaknesses. For example, enterprises might have commodity IDS or AV software. But those protect only against malware with known signatures. Furthermore, those standard defense systems are worthless once an attacker gains network access using stolen credentials.

Manage third-party vendor access

Attackers routinely compromise organizations by entering their environment through one of their business partners. So network access needs to be carefully managed for third-party vendors based on their roles and duties. Your outside financial auditing firm, for instance, should have different access to your network than the company that delivers office supplies. Working with clients, we frequently see organizations that have overly permissive access policies.

One of the most notorious third-party vendor breaches occurred in 2011. The initial victim was an outsourced service provider. Before the attack was over, cyber criminals had stolen sensitive customer information from more than 50 major companies.

Regardless of the significance of the vendor to your organization, you have to make sure that their "papers are in order" when they access your network. All the perimeter security in the world won't protect you if an attacker passes through the checkpoint with stolen credentials.[5] You need to risk-rank your vendors and your own people. You need to verify what security the vendors have in place to catch stolen credentials. You also need to monitor their access 24/7. If your employees usually log in between 9:00 a.m. and 5:00 p.m., you have to ask why someone's logging in at 3:00 a.m.

[5] Mathew J. Schwartz (InformationWeek). "Epsilon Fell To Spear-Phishing Attack." April 2011.

Attackers routinely compromise organizations by entering their environment through one of their business partners. So network access needs to be carefully managed for third-party vendors based on their roles and duties.

Provide a security architecture

Thoroughly understanding your security architecture is critical to determining how well various systems work together and whether security gaps present a risk.

We often find that clients have made certain security investments in the name of compliance, not security. In some instances, clients have installed new firewall, IDS or AV technology to comply with Sarbanes-Oxley, a U.S. law governing public companies. They believe they're safe because they're compliant — but one doesn't always follow the other. Some companies may keep logs of network activity but never look at the logs to detect anomalies.

If a company invests in the latest security technology but doesn't monitor it and build a process behind it, the money is wasted. You can buy all the silver bullets you want and put them in your gun, but if you don't fire it, it doesn't matter.

You need to determine whether your security is up to date because security technology is always evolving. You also need to update your architecture for emerging technology such as cloud computing and mobile devices.

Managing infrastructure sometimes reveals a gap between the IT and security teams that's as wide as the gap between IT and the business side. IT is all about performance and capabilities, not security. When your security team comes along to point out the security flaws to IT, they often come off as the bad guys. It's like a design team focusing on how to make a car that goes from zero to 60 in eight seconds — and all security is concerned with are the brakes, air bags and seatbelts.

If you identify tools that are out of date or are no longer needed (such as unused network ports), remove them. They can clutter your network and present an opening for hackers.

Make your infrastructure resilient

If you do suffer an attack, ensure that your critical resources remain available even as you manage through the breach. For some of our clients, it's a much bigger issue than making sure your e-commerce site stays up.

Some of our clients are airlines whose flight operations centers are critical to keeping flights on schedule, planes in the air and passengers safe. The operations centers must be built for high availability and simply cannot go down even if infected by malware. In those situations, an airline needs a backup or secondary system that can continue operations while the security team fixes the breach. Furthermore, the incident response team has to know which systems they cannot disable while responding to the event.

Distinguishing between disaster recovery (DR) and business continuity planning (BCP) is crucial. A security company delivers DR, which means their technology and services discover a security incident, warns of it, responds and works to remediate the situation. BCP, on the other hand, is the responsibility of the company to put systems in place so that the business goes on as normal in spite of a breach.

One approach to business continuity planning is to establish a mirror data center that replicates data from the main data center in real time. That way, if you have a security incident that takes down several servers for a few hours, the business can keep going through the mirror data center.

Keep security top of mind

Your employees are your first line of defense. Instill in them the same "If you see something, say something" attitude of security that exists in the physical world. Maintaining a successful security profile is about remaining vigilant. That means offering targeted training for incident response teams based on their roles.

The rank-and-file might dismiss continuous training as a boring annual obligation, a box to check off and forget. Encourage them to view it as keeping skills sharp. You also need to be open to revising policies or creating new ones as best practices evolve. Reminding employees to keep security top of mind every day is vital.

STEP THREE: CONDUCTING A SECURITY PROGRAM ASSESSMENT

Gathering information across the ten areas outlined in "Step Two: Evaluating Your Security Program" typically takes about six weeks. While some organizations do this on their own, many engage the help of a third-party consultant. Regardless of how you choose to conduct your assessment, consider the approach outlined in the following sections.

Collect and analyze currently deployed requirements, practices and technologies

In a security program assessment, consultants and staff review existing security policies, standards and procedures to identify current operational capabilities. This process should look at what types of security technology you currently deploy and compare it to the state-of-the art technology and industry standards. If you had a recent breach, providing details about the event to the assessment team is important. Reviewers should interview key stakeholders about the company's security posture.

Bring in all stakeholders

Get input from C-level executives, security staff, rank-and-file employees and other stakeholders. One useful exercise is to have interactive sessions with various groups of employees to generate ideas, answer their questions and develop a strategy.

One firm ran a security drill with a room full of employees, including a security director. Then, the security director left the room, and the remaining workers had to fend for themselves, with disastrous results. Lesson learned: some security roles should not rest with just one person. What if she's on vacation that day?

Top executives, directors and other employees on the business side may come to the security debate with a different point of view from those focused only on IT security. And people on the business side will be comparing their security to that of their competitors. This is where the critical "How secure do you want to be?" question comes up. You have to decide whether you want to simply comply with minimum security requirements, match those of your competitors or gain a competitive advantage by exceeding what they have.

Build consensus

An important outcome of the assessment is that management continually builds consensus among all parties to support the final plan. The business side and IT may have differing approaches and priorities. IT and security may even have competing needs. But everyone needs to agree on the best approach to accomplish the goals of the assessment and the roadmap: making the enterprise as secure as it can be.

You have to decide whether you want to simply comply with minimum security requirements, match those of your competitors or gain a competitive advantage by exceeding what they have.

Present the roadmap

The assessment process typically culminates in a two-year roadmap — plus or minus a year, depending on your situation. This roadmap establishes project priorities based on the urgency of a particular weakness and available budget. It lays out short-, medium- and long-term goals. And it looks at capital expenses (CAPEX) and operating expenses (OPEX) needed to implement the plan.

While we've mentioned instances of clients who get sticker shock when we tell them how much a security upgrade will cost them, sometimes the opposite occurs. One client was a janitorial services firm that presented an aggressive security upgrade plan we thought was a case of overkill. We told them they don't have the same risk profile as their customers in financial services, aerospace or government.

Prioritize security improvements

The timeline for implementing that roadmap has to be created with input of C-level executives and can be a challenge. The chief information officer (CIO), chief information security officer (CISO) or a security manager may understand the details of each of the recommendations, but the CEO, CFO, directors or others may not be on the same wavelength. Many times, executives outside of IT are surprised by the number of initiatives in the report and the effort and financial obligation it will require of them.

FIGURE 3: THE SECURITY ASSESSMENT PROCESS

CONCLUSION AND RECOMMENDATIONS

A security program assessment follows a logical sequence of steps to help you answer the question "How secure do you want to be?"

It starts with assessing your current situation based on 10 key areas, designing solutions to address the issues in your environment, creating a clear roadmap to transform your organization and continuously monitoring to help sustain your secured environment.

A big part of sustaining your secured environment is to remain vigilant about new and emerging threats. As enterprises develop security to block malware, cyber thieves and denial-of-service attacks, the bad guys are constantly developing new ways to wreak havoc. Today, it's not enough to look for attacks that have known signatures; security must evolve to the point where it studies network traffic that may have the makings of a malicious attack.

The assessment process helps all the top decision makers in an organization become more aware about security issues and understand the implications of a breach. It's not just about your site or some servers going down. It's about lost sales, stolen trade secrets and the substantial costs of remediating the attack. More importantly, it's about the damage to your reputation if the news of your breach hits the national news.

When deciding whether or how much to invest in a security program assessment and implement recommended changes, consider this: attackers are constantly innovating. Ask yourself if you should be innovating, too.

HOW MANDIANT CAN HELP YOU

The Mandiant Security Program Assessment offering draws on technical and investigative skills developed over the course of hundreds of thousands of hours on the front lines. We have a front-row seat to security programs that attackers have evaded, which provides a unique perspective when advising organizations on how to evolve their own programs.

Mandiant consultants have also built and run some of the world's biggest security programs, including preeminent names in technology, law enforcement, entertainment, retail and government.

For more information about the Mandiant Security Program Assessment, visit our website:
https://www.fireeye.com/services/mandiant-security-program-assessment.html

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

www.FireEye.com

FireEye