ACHIEVING SECURITY MATURITY: A ROADMAP TO BUILDING A ROBUST CYBERSECURITY CAPABILITY
INTRODUCTION

One of the fundamental characteristics of any mature organization is self-awareness. To be effective, this concept should permeate the entire workforce, from the CEO down to the hourly employees. Understanding what your organization does well and how to continue it, and knowing what you don’t do well and how to fix it, are essential to building and sustaining a successful enterprise. This awareness is even more critical when it comes to your cybersecurity program.

In this white paper, you will learn what it means to build and maintain a mature cybersecurity program. You will also receive guidance on how to continuously improve your program so that your security maturity level evolves to meet tomorrow’s challenges.
At the heart of these questions is an attempt to provide the most relevant information to an organization at the appropriate time. If you buy a used car, you want to first make sure it is fundamentally safe before worrying about whether the paint is chipped. The last thing you need is to roll down the highway with a new ruby red coat reflecting the sun while mashing brakes that don’t function. To progress in a meaningful and sustainable manner, you must understand your priorities and how your maturity level is dictated by your own circumstances, while also influenced by those of your industry as a whole.

These questions are not mutually exclusive — each builds on the next. In the experience of the CrowdStrike Services team, the organizations that plan and prepare to address issues proactively can reduce their attack surfaces, while simultaneously reducing the risk of a damaging and compromising breach.

**AM I BREACHED?**

As a trusted advisor to leadership teams, CrowdStrike always recommends that you make sure your house is clean before you welcome guests. If your defenses have already been breached and an adversary is dwelling in your systems, the actions you take to mature your capabilities are likely to fail — because that adversary is observing and counteracting your defense measures with each step you take.

Therefore, the first part of maturing your cyber defenses is to discover if you have already been compromised. Leverage not only current incidents, but those that occurred previously in your organization and in your peers’ organizations. This information will allow you to develop a better sense of self-awareness and also a strategic approach to your future security program, marked by increased maturity across key functions and the ability to exercise those capacities on a recurring basis. Undertaking a compromise assessment is key in this endeavor.

First and foremost, a compromise assessment is designed to identify current and/or past attacker activity in an environment. Second, it allows organizations to discover activities that reflect poor IT hygiene, such as crypto-mining, extensive use of administrative or security technologies, or non-standard tooling for things such as VPN, remote access or multi-factor authentication (MFA). This type of threat-hunting exercise requires experts with the skills and experience of many years of hunting and responding to the most sophisticated intrusions around the world, combined with powerful and innovative detection, analysis and forensics tools. All of this is focused on addressing the critical question: “Has my organization been breached?”

When the goal is to find evidence of a breach, organizations should be prepared to deal with that information when it surfaces. CrowdStrike has worked with some organizations that, to put it bluntly, were not prepared to answer the call when the results were delivered. In these situations, customers felt that the compromise assessment revealed too much about their security posture — or lack thereof. For others, finding evidence of a targeted attack was the goal, and they then relied on CrowdStrike to support them in removing that threat.

A side benefit of conducting a compromise assessment is deploying an endpoint security technology such as the CrowdStrike Falcon® platform. When a threat is identified, Falcon
provides an organization with near real-time visibility into the malicious actor’s current activities. In addition, Falcon allows organizations to contain these threats more quickly. What takes some organizations weeks or months, Falcon is able to do in days, if not hours: Identify the threat, contain the infected machines and leverage prevention policies to keep the attack from recurring. It’s important to make sure you’re working with an organization that not only has the ability to perform incident response (IR) but also has the proper technologies to support it.

AM I MATURE?

If your self-inspection into cybersecurity breaches reveals that there is no evidence of compromise, consider yourself lucky. However, do not consider yourself lacking in areas for improvement in enhancing your defenses even further. Even organizations with the most mature cybersecurity capabilities are constantly evolving and looking for ways to improve. But the initiatives that a Fortune 50 financial institution is following should not be the same as those of a smaller regional retailer. Maturity, while generally following the same scale, requires different targets based on a company’s profile. This profile should include both threat information and risk posture. As the industry shifts, so should corporate goalposts for cybersecurity.

CrowdStrike categorizes a cybersecurity program according to six key areas:

1. Security foundations
2. Prevention, detection and response
3. Governance
4. Threat intelligence
5. Simulation exercises
6. Hands-on operations

Collectively, these categories support each other, while also being important in their own right.

SECURITY FOUNDATIONS

When speaking of security, it’s important to delineate between cybersecurity and information security. Often, these terms are used interchangeably, but they are not the same concept. If you consider information security to cover anything that protects information, then you realize it spans both the physical and cyber worlds. Consequently, information security encompasses many areas that are vital to an organization’s overall health and wellness but fall outside of the world of cybersecurity. This distinction is important when considering maturity. Updating out-of-date systems, installing patches and managing end-of-life devices are all part of a broader information security program of an organization, whereas these fundamental activities are the bedrock of a mature and successful cybersecurity program.
PREVENTION, DETECTION AND RESPONSE

Beyond basic security foundations, the core capabilities in a cybersecurity program revolve around prevention, detection and response. Ask yourself:

- What is your ability to prevent breaches from happening in your environment?
- Knowing that you can’t prevent every instance, how well are you able to detect and respond to those breaches that slip through?

One of the most difficult things for people to understand about a cybersecurity event is that it’s inherently very different from other incidents in your organization because it’s constantly evolving. Moves and countermoves with an attacker on the other side of the breach are akin in many ways to physical warfare. To counteract this level of sophistication, it’s essential to invest in prevention, detection and response capabilities at three levels: people, processes and technology.

These three areas are discussed in most cybersecurity maturity assessments and for good reason — any two without the third results in failure. Without the appropriate staffing, a tool becomes “shelfware.” Without the necessary processes in place, functionality is inconsistent and unrepeatable. Without the right tools, you’re bringing a sword to a gunfight. But together, these three concepts applied across your organization’s prevention, detection and response functions allow for the flexibility and ability to counteract a cyberattack, albeit at differing levels based on maturity. The ultimate objective in undertaking a cybersecurity maturity assessment is to ensure you are mature enough to withstand and respond to the most advanced adversaries you are likely to face. One more thing to bear in mind is that maturity is not a given — it has to be worked at. Cyber “muscle memory” has to be trained for and exercised and if it isn’t, then atrophy is a real danger that can weaken an organization facing lean and capable adversaries.

GOVERNANCE

The ability to prevent, detect and respond to cybersecurity events is predicated on the idea that you can do so in an ongoing, repeatable manner with support across the organization. The implementation of robust and thoughtful governance and threat intelligence allows an organization to move beyond the initial maturity levels of its cybersecurity program.

One of the quickest ways for a cybersecurity program to fail is for it to operate without the support of others in the business, especially those in leadership positions. With today’s constant barrage of headlines about cyber breaches, cyber risk is typically at the top of every board’s agenda. However, a lack of understanding combined with heightened awareness often leads to a well-intended but poorly executed program. It’s not uncommon to get funding for a required tool but no additional funding to hire staff to monitor and administer the tool.

With the ever-changing threat landscape, organizations must continuously evolve their governance capabilities. For most, this requires developing playbooks to be used in response to a cyber incident. CrowdStrike helps companies design playbooks to improve their incident response operations by standardizing and streamlining processes across the organization. CrowdStrike analyzes current plans and capabilities and then works with the company to develop relevant processes and documentation, including incident response plans, policies and/or playbooks.

THREAT INTELLIGENCE

The decision to invest in cybersecurity should be driven not only by what you think is valuable within your organization but also by an understanding of how that data and information are valued from an external perspective. These views are not always aligned and it’s always eye-opening to hear “I don’t have anything that anyone would want.” If you find yourself saying this, you likely haven’t assessed your assets from a threat actor’s point of view.

To this end, CrowdStrike looks at an organization’s threat intelligence capability as the final element of an effective security program. In short, threat intelligence can be used to enhance prevention, detection and response capabilities, inform a robust governance model and ensure that basic security foundations are being addressed in a meaningful way. While it’s uncommon to find a mature threat intelligence capability in most organizations, the companies that aim to anticipate threats will leverage intelligence to give themselves an edge.
AM I READY?

After confirming that you don’t have an active adversary in your environment and maturing your cybersecurity capabilities, the next step in evolving your program is practice. Even though you will never achieve perfection, it’s possible to respond effectively to a cyber incident with less-than-perfect capabilities — but choosing the right practice method depends, again, on your maturity.

There are two primary exercise types in the world of cybersecurity: simulated exercises and hands-on operations. Within these categories, there’s quite a bit of variance, allowing an organization to dial the complexity up or down and fine-tune other levers to ensure the desired goal is achieved.

SIMULATION EXERCISES

The primary goal of a simulation exercise is to allow a group of people to collaboratively respond to a fictitious scenario. The participants are able to walk through a cyber incident without having to actually experience one in real life. This walk-through is most often a tabletop exercise. Collaboration during these sessions allows for valuable discussions on points of disagreement, all occurring in a safe environment. This format also allows participants from other areas of the business to provide input on a topic that may typically be handled by a different department — for example, the CFO may have input into the communications plan.

Other goals of a tabletop exercise include highlighting inefficiencies in internal processes, bringing together employees from across the organization who would not otherwise interact, educating participants about relevant cyber threats facing the organization, revealing gaps in security controls and highlighting the impact that those gaps could have during an attack. Through a tabletop scenario, it’s possible to achieve all of these goals.

Separately, the scenario itself can be tailored based on the maturity of the organization. For a group that has never talked about a cyber incident, it may be helpful to simply walk through small scenarios alongside an IR plan, offering guidance on which roles certain individuals would play in the response. As an organization matures, the scenarios should get progressively more difficult, placing the burden on individuals to come up with decisions when the IR plan may not offer all of the answers.

An offshoot of the tabletop exercise is the “live fire” exercise (also known as a cyber war game). This model relies on role playing and realistic attack scenarios more than collaborative discussion and single-threaded events. Individuals are put in a position to prove — or disprove — their understanding of cybersecurity incident response while responding to events and data as they would in real life. The value here is the realism factor. Rather than discussing a hypothetical call, the CISO may need to actually pick up the phone and listen to a role-playing “journalist” describe what has been learned about the attack.

Generally, the live fire exercise should be conducted in organizations that have very mature cyber capabilities and with individuals who have gone through simulations before. Without prior knowledge and experience, individuals risk looking bad in front of their peers — never the purpose of an exercise.
HANDS-ON OPERATIONS
While simulation exercises revolve around discussion, hands-on operations involve technical response. Whereas a tabletop exercise is known to participants ahead of time, most “red team” exercises, such as an adversary emulation, are conducted without the advance knowledge of the teams responsible for responding to the simulated attack. In its purest form, an adversary emulation involves taking on the role of an advanced threat actor and attempting to gain access, move laterally, elevate privileges and ultimately achieve the goal of the test — which is typically gaining domain admin rights, accessing a sensitive area of the network, accessing restricted data or carrying out another malicious action.

Depending on the goals of the organization, this type of test may include social engineering, spear-phishing, physical security tests, WiFi tests and more. While the red team’s goal is to achieve its objectives without being detected, there’s also value in observing an organization’s capabilities at each phase of the attack. Simply detecting an attacker in the network doesn’t prove one’s maturity. The true test is whether you can stop an adversary from achieving its objectives before you remove it. For this reason, it’s important in a red team exercise to test not only tooling but also the people and processes behind those tools. Again, this highlights the central trinity of cybersecurity capabilities — prevention, detection and response.

Many organizations are expanding these real-time training opportunities by including a blue team as well. In this red team/blue team (or purple team) model, a dedicated blue team member sits with the responders and shows them how they could have detected the red team activities through various log sources, tools or technologies. Rather than waiting for a report at the end of the adversary emulation, responders learn right away as they see the results of the red team attack in their tools as it occurs.

WHAT SHOULD I AIM FOR IN MY CYBERSECURITY PROGRAM?
The CrowdStrike Services Team hears this question often, and the answer varies. The team addresses this question through the prism of what CrowdStrike calls “breakout time” — the window of time from when an adversary first compromises an endpoint to when it begins moving laterally across the network. Based on telemetry data gathered by CrowdStrike in 2018, the overall average breakout time across all intrusions, threat actors and regions in 2018 was 4 hours and 37 minutes.

Threat profiles and organizational imperatives will vary, but in general, your cybersecurity program needs to move at the speed of the adversary. The CrowdStrike approach recommends that an organization should be focused on implementing the “1-10-60 rule.” This rule requires you to detect an incident or intrusion within one minute, determine if the incident is legitimate and decide on next steps within 10 minutes and remediate the incident by ejecting the intruder and cleaning up your network within 60 minutes.
You need to be building, maturing and assessing the people, processes and technology that underpin your cybersecurity program with the goal of operating according to the 1-10-60 rule, as this guideline is the best guarantee of staying ahead of the adversary and stopping a potential breach from occurring. It may not be the right target for all organizations, but it helps gauge the quality of a mature cybersecurity capability.

ABOUT CROWDSTRIKE SERVICES

CrowdStrike Services equips organizations with the protection and expertise they need to defend against and respond to security incidents. Leveraging the cloud-delivered CrowdStrike Falcon® platform — next-generation endpoint protection, cyber threat intelligence gathering and reporting operations, and a 24/7 proactive threat hunting team — the CrowdStrike Services security team helps customers identify, track and block attackers in real time. This unique approach allows CrowdStrike to stop unauthorized access faster and prevent further breaches. CrowdStrike also offers strategic advisory services so organizations can improve their ability to anticipate threats, prepare their networks, and ultimately stop breaches.

ABOUT CROWDSTRIKE

CrowdStrike Inc. (Nasdaq: CRWD), a global cybersecurity leader, is redefining security for the cloud era with an endpoint protection platform built from the ground up to stop breaches. The CrowdStrike Falcon platform’s single lightweight-agent architecture leverages cloud-scale artificial intelligence (AI) and offers real-time protection and visibility across the enterprise, preventing attacks on endpoints on or off the network. Powered by the proprietary CrowdStrike Threat Graph, CrowdStrike Falcon correlates over 3 trillion endpoint-related events per week in real time from across the globe, fueling one of the world’s most advanced data platforms for security.

With CrowdStrike, customers benefit from better protection, better performance and immediate time-to-value delivered by the cloud-native Falcon platform.

There’s only one thing to remember about CrowdStrike: We stop breaches.

Learn more: https://www.crowdstrike.com/