LOCKHEED MARTIN

A False Sense of Cybersecurity
Three Pitfalls to Avoid

A White Paper Presented by:
Lockheed Martin Corporation

A False Sense of Cybersecurity; Three Pitfalls to Avoid

Breaches disclosed in the media foster conversations within organizations on how to protect critical assets. Loss of intellectual property, financial data and consumer confidence have produced tangible evidence of an evolving threat landscape that, in turn, has elevated cybersecurity conversations to the board room. Security executives tasked with preventing their organization from being the next news soundbite are getting more support and more budget than ever before.

This cyber awakening has many organizations evaluating current security measures including tools, people and processes. However, it's critical to refer back to the overarching strategy: achieving cybersecurity maturity. The conversations within our organizations have evolved, but are the investments we're making truly protecting us against today's sophisticated adversaries? Are we being lulled into a false sense of cybersecurity?

> *Organizations are not prepared to deal with severe and frequent cyberattacks.*

Lockheed Martin recently sponsored a Ponemon Institute survey of 678 U.S. information technology (IT) and IT security practitioners familiar with their organizations' defense against cybersecurity attacks and with responsibility for directing cybersecurity activities. When asked about the challenges of achieving a strong cyber defense, 75 percent of respondents indicated an increase in the severity of cyberattacks and 68 percent said they are more frequent than ever before. Although a majority attest to the increase in frequency and severity of cyberattacks, only 53 percent believe that a strong offense is very important to their security strategy. Employing an offensive approach to cyber threats requires a mature security posture. A four-point cybersecurity maturity scale measurement of 0.5 – 1.0 indicates a good basic network security hygiene and 3.5 – 4.0 identifies a mature, Intelligence Driven Defense® framework. Many organizations find themselves in the 1.5 to 2.0 reactive posture range.

Are our misconceptions of our technology, staffing and/or processes keeping us from taking an in-depth look at the effectiveness of our cybersecurity program? Are we taking actions that will mature us into a proactive or even predictive approach?

Be wary of three common mistakes often made when advancing an organization's cybersecurity program and the appropriate actions you can take to avoid them and better protect your critical assets.

Pitfall #1: Alerting tools will defend your organization.

Security operations centers are often designed with technologies meant to alert network administrators when bad things are happening. Traditionally, organizations have bought (literally bought) into the idea that there is a mix of technologies that can be plugged into the network to detect all potential issues and intrusions. Heavily investing in tools "that go bing" to defend a network is what we call a vendor-driven response model.

> *According to a survey conducted by Lockheed Martin at the 2015 Gartner Security & Risk Summit, nearly 40% of security professionals identified "technology," including alerting tools, firewalls and SIEMs, as contributing to their level of confidence when it comes to securing their enterprise against cyberattacks.*

To avoid this pitfall, it's critical to understand that there's no such thing as a silver bullet for cybersecurity. You can't buy your way into becoming a secure organization, and the traditional set-it-and-forget-it approach doesn't work.

Preventing a large-scale attack from striking is like finding a needle in a haystack. Advanced and focused attackers employ techniques designed to bypass traditional security technologies. Defense efforts limited to only vendor-driven detections and out-of-the-box solutions often miss the evidence. Security technologies in place (AV, firewalls, IPS, IDS, etc.) can effectively reduce the noise and diminish the size of the haystack, but in order to find the needle and prevent a large-scale attack tools need to be customized. This will ensure they generate meaningful alerts based on your unique environment and designed to protect your unique assets.

A second survey conducted by Ponemon Institute in April 2015, Risk & Innovation in Cybersecurity Investments, explored the return on investment of cybersecurity. An overwhelming 90 percent of respondents said their organization invested in a security technology that was ultimately discontinued or scrapped before or soon after deployment.

"As cyber threats increase, it is troubling to see so many cybersecurity tools purchased by organizations end up as shelf ware," said Greg Boison, a director of Homeland & Cybersecurity at Lockheed Martin. "When cyber dollars are scarce, organizations should not only evaluate which tools their enterprise needs, but whether they have the internal and external resources to deploy, maintain and leverage them."

Organizations deemed most innovative have found ways to use existing technologies to implement more efficient and cost-effective security.

The reality is there's no one solution that will serve all your cybersecurity needs. Beware of stocking up on technologies that foster undue confidence resulting in a false sense of cybersecurity. **Alerts will always outpace the analyst's ability to respond, and off-the-shelf technology never satisfies all cyber defense mission needs.**

Avoiding This Pitfall

Measure your maturity. A response-driven posture is not going to have impact in today's evolving threat landscape. Waiting to be told there's a problem can cost you. Even if you survive the firefight, you often come away with nothing—no intelligence to help protect from future attacks and no time to truly debrief and grow before another alert is sounded and you're back in the fight. A response-driven posture is not sustainable.

Assess your tools. Assess tools against threats that target your most valuable assets. Technology is a necessary part of the equation but you don't need to accept the status quo—technology should be tuned to work for you. The hardest part of analysis is actually getting good data. Tune your tools and capabilities in your enterprise to collect good data.

Find ways to leverage intelligence. Disable the out-of-box alerting and tailor the settings to fit how your people work. Properly tuned tools collect good data and can shift a team's day-to-day tasks from merely reacting to alerts to focusing on truly analyzing relevant data to affect thoughtful defense.

Pitfall #2: Security is attained through 24x7 staffing.

Detecting and containing advanced threat actors is extremely difficult without humans in the loop. However, we want to dispel the idea that a 24x7 staffing model equals security. What we often see in the marketplace is that organizations with 24x7 staffing think they're covered. They overestimate the security maturity gained by the headcount, and they aren't asking the right questions about their program's effectiveness.

- Do we have enough skilled cyber analysts to fill a 24x7 staffing plan?
- Is the staff manning each shift equipped and qualified to react and mitigate threats or are they serving as a manual escalation trigger to alert key staff?
- Could technology be tuned and customized to alert and escalate when key events are detected?

Quality vs. Quantity Staffing

The Ponemon Intelligence Driven-Defense Cyber Survey reported that "56 percent of organizations […] operate a fully staffed 24/7/365 schedule. Respondents are evenly divided on whether such staffing is necessary in order to have a strong cyber defense."

We view cyber staffing models as a skewed bell curve—it starts out low, grows quickly as it approaches peak staffing levels, then tapers off as the SOC reaches higher levels of maturity. Three-shift coverage models are difficult to staff and even harder to staff with qualified cyber analysts, typically resulting in an under-utilized, less capable crew on night shift.

> *Lockheed Martin survey results reveal staff turnover is up to 50 percent in the past 12—18 months.*

The standard solution to this problem across the industry has been a "follow-the-sun" model; but unless you're a multi-national corporation or willing to outsource your SOC, this is both difficult and cost-prohibitive. Given the limited cyber resources in the market today, staff hired for second and third shifts are more likely to be tasked with manually alerting first-tier analysts when an incident is detected. This function is equivalent to designing systems and programming technology to alert via cell phone, email or a service desk. Having a highly tuned infrastructure aligned to only alert for critical issues can produce the same results at a fraction of the cost.

If your sensors are tuned with the appropriate detections, alerts are configured properly according to severity, and you have complete network visibility (admittedly a tall order), there is no compelling reason to staff the SOC 24x7x365. In the end, it comes down to staff quality, rather than quantity. Most SOCs focus on staffing numbers when they first start out, missing the tried-and-true lesson that a rock star analyst is worth three less-skilled peers.

When is 24x7 coverage appropriate? Sometimes. For example, there will be times that the SOC should be staffed around-the-clock, such as during a major incident or particularly active times in threat-actor cycles. Also, staffing a SOC 24x7 can benefit while fulfilling industry compliance requirements such as continuous monitoring. Accordingly, many utilities and financial institutions see the prevailing value in 24x7 eyes-on-glass monitoring.

In many cases, 24x7 staffing is required for compliance, by corporate direction or by senior leadership. Discussion should be focused around how to transition to an environment where 24x7 is not required. To do so, technologies must be automated and tuned to identify a priority alert vs. one that can be postponed. This comes with time and maturity, so a transition from 24x7 to 16x7 to 14x5 is something organizations should strive for to maximize resources.

The Follow the Sun model is another example of large organizations addressing the issue of staffing a third shift. As we know, great challenges related to resource maximization and extracting value from analysis come with that shift. This model might be an alternative to staffing three shifts.

No matter what you decide is the right staffing program or schedule for you, **make sure you're accomplishing something. You could be doing 24x7 and accomplishing zero if you're not asking the right questions about your program.**

Avoiding This Pitfall

Question the effectiveness of your staffing plan. Evaluate and look for ways to customize and tune your technology to enable quality alerting.

Explore the benefits of tuning technology for effective escalation. Do you have skilled analysts or manual alerting? If skilled cyber resources are limited, use them wisely. Could you tune your technology for quality alerting?

Leverage intelligence to identify trends in the timing and/or cadence of attacks to inform your staffing decisions and your training plans.

Pitfall #3: No Framework

What we consider "no framework" some organizations might actually point to as their strategic framework—waiting for something to happen and then reacting. This could be a planned strategy or just the reality of your current operations. But not having an evolved, sustainable and scalable framework is a pitfall that plagues many organizations.
Actually, having no framework directly contributes to the first two pitfalls: technology and staffing.

Technology: When you don't have a framework you buy more things that wind up as shelf ware. A framework is an imperative to help you analyze your technology choices. If I have a good framework I have good metrics to measure the effectiveness of technology investments or gaps in service. Lockheed Martin developed the Cyber Kill Chain® security framework to thwart cyber threats. By analyzing the Cyber Kill Chain solutions Cyber Threat Model, LM analysts are able to successfully prevent cybersecurity breaches. This approach supports an ability to measure the effectiveness of technology based on how it performed during known attacks. Informed decisions are then made based on intelligence to eliminate or tune tools that are underperforming or not performing.

Staffing: If you don't want to fight fires, ensure you have to have a framework within which you can operate efficiently and intelligently. Most organizations are doing event-by-event inquisitions rather than taking a proactive approach to cybersecurity. The Lockheed Martin Cyber Kill Chain® framework was developed to guide thinking about network defense, adopting the mindset of the adversary and integrating those thought processes with our own to defend the network and become more proactive.

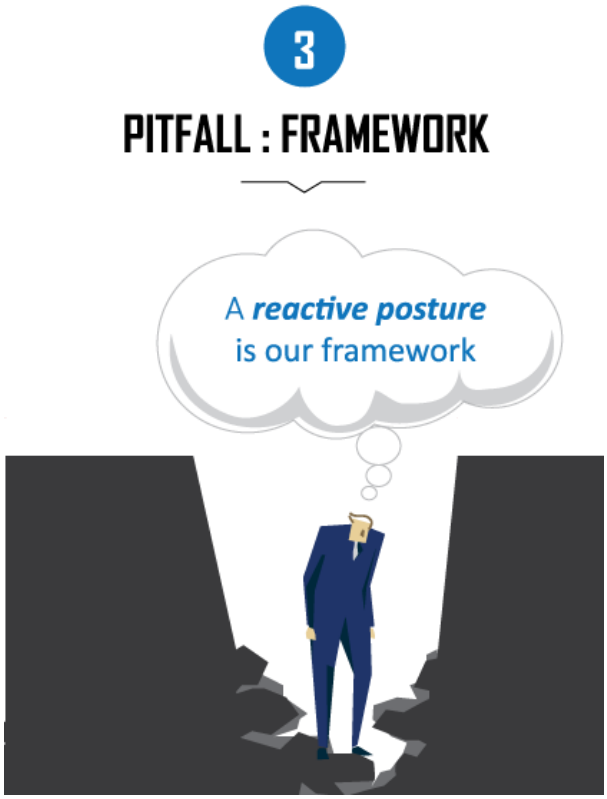
Good intelligence begets good intelligence; you learn something and use that knowledge in collaboration with others, and you learn something else. This is an ongoing cycle where you're keeping up with—if not ahead of—your adversaries, never left behind. Gone are the days of firefighting.

Make sure your corporate network is designed in such a way that it's defendable in the first place. The cyber architects triad promotes resiliency through visibility, manageability and survivability.

- How many internet gateways are there?
- How do we process email?
- Do we have the availability to have visibility into all phases of the Cyber Kill Chain® solutions Cyber Threat Model cycle as they affect our network?

Processes and procedures have historically been viewed as simply an audit requirement. Once compiled they remain shelved and unused. However, the development of the foundational requirements to operate a successful, world-class SOC requires the establishment of effective documentation to drive operations.

Processes and procedures need to be enablers designed to assist cyber analysts in applying their analytical prowess in advancement of the objective—that of solving complex problems. A proper framework should be interactive and provide analysts with ideas and concepts that can be leveraged during their investigative analysis phases. Processes should be viewed as a reference and knowledge transfer resource with clear and standardized workflows to ensure consistent results and foster an environment for continuous improvement.



Avoiding This Pitfall

Evaluate your framework. A reactionary posture is not a mature or sustainable framework. To mature your organization you must first make an honest assessment of your current processes and procedures. Consider evaluating yourself against a proven framework with demonstrative results advancing other organizations.

Rethink network architecture in the context of cybersecurity. Corporate network architecture needs to be designed in a defendable way to promote resiliency through visibility, manageability and survivability.

Adopt a framework that leverages intelligence. Track, trend, analyze, and collaborate. Be proactive.

Conclusion

Cybersecurity is being socialized on an unprecedented scale and it's getting the attention of the boardroom.

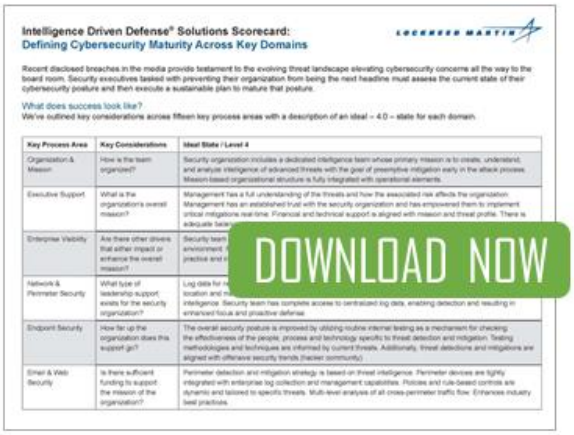
> *In Lockheed Martin's recent survey, 62 percent of respondents indicated that their cybersecurity budgets have increased up to 30 percent in the past 12—18 months.*

The question is how you can maximize your budget to ensure your organization is protected. Today you have the perfect opportunity to engage and educate your organization to address the cybersecurity maturity of your environment. Now is the time to assess the tools, processes and procedures currently in place thoroughly examining if they are accomplishing the goal to defend against sophisticated threats, protect the enterprise, and scale to meet the demands of the future. That's the journey Lockheed Martin embarked on over a decade ago—we've adapted to the evolving landscape and developed technologies, skill sets and tradecraft to enable the Intelligence Driven Defense® methodology across our enterprise.

Watch where you're running. The three common pitfalls are common for a reason. The increase in disclosed breaches has opened up a cybersecurity maturity dialogue across organizations worldwide. Now is the time to question how we've done things and how we're doing things: Is the status quo enough or have we been lulled into a false sense of cybersecurity?

Leverage intelligence so you're not lulled into a false sense of cybersecurity.

- Adopt a framework driven by intelligence.
- Build a team to leverage information within that framework.
- Tune your tools to collect and aggregate intelligence your team needs to operate within the framework.



What does success look like?

We've outlined key considerations across 15 key process areas with a description of an ideal 4.0 state for each domain.

Click to download our 4.0 cybersecurity maturity scorecard >

For more information on cybersecurity solutions
Email: cyber.security@lmco.com
Phone: 855-LMCYBER (856) 562-9237
www.lockheedmartin.com/cyber

Version 1.0
PIRA#CMK201507001