OPERATIONALIZED SECURITY FOR A SAFER GOVERNMENT

Industry Perspective

FireEye

Executive Summary

There's a common saying that if you build a 10-foot wall, someone will show up with an 11-foot ladder. Especially in cybersecurity, that idiom rings true. Even as organizations install new firewalls, patches and other network security tools, hackers are constantly developing new ways to infiltrate those defenses.

How is the government supposed to stay ahead of these increasingly sophisticated cyberattacks? In an interview with GovLoop, Tony Cole, Vice President and Global Government Chief Technology Officer at FireEye, explained that the answer lies in the concept of operationalized security.

FireEye provides a unified suite of defense solutions that helps organizations engrain security into every facet of their technology and operations. "Security can be very complex, but if you put the right policy, processes and tools in place, and continuously learn from that, you actually end up removing some of the complexity from that environment," Cole said.

In this industry perspective, we'll explore how to create those appropriate policies, processes and tools with the help of a trusted solutions provider. We'll explain why agencies are currently struggling to counter advanced attacks, how they can learn from their environment and what they need to evolve their defenses. Finally, we'll investigate how operationalized security can create a more secure government.

A Lack of Awareness

Shrinking budgets, legacy IT systems and cyberattacks escalating in both volume and sophistication all challenge agencies to secure their infrastructures. But there's an even bigger obstacle at many organizations, Cole said. "You could talk about challenges for hours, but I would say the largest challenge in this space today is people not understanding the scope of the cybersecurity problem in our interconnected systems," he said.

While most government employees understand the broad implications of a security breach, Cole said many public servants aren't aware of the specific risks at their agency. When organizations lack clear targets for cyberattacks – like classified intelligence information or citizens' financial data – it's easy for employees to assume their agency isn't at risk. As a result, they don't take measures to buffer protections and safeguard information.

That isn't to say that organizations don't have any cybersecurity protections. Instead, Cole said many agencies simply rely on outdated systems, processes and architectures that can't mitigate today's sophisticated attacks. That's a problem for both IT managers and the information systems they manage and should be a major concern for agency leadership.

To remedy this lack of awareness, Cole suggested starting with real-time information sharing within government. Agencies can start by reaching out to similarly sized organizations with related missions. Trusted third-party vendors like FireEye can facilitate these conversations where connections don't currently exist. Particularly if the advising agency is more advanced in its cyber defenses, conversations over shared vulnerabilities and threats can help illuminate new attack vectors or targets for newcomers to cybersecurity.

To really confront the threat landscape at an individual agency, however, requires more than information-sharing. It will require an in-depth and ongoing assessment of your current systems, threats and processes that can inform a better, unified defense strategy. That unified defense is called operationalized security.

Assess Your Organization Before Operationalizing Security

Because many agencies rely on tools that don't meet current needs, the first step to operationalizing security is actually not to start implementing changes for the future. Instead, take the time to assess the current threat landscape of your agency related directly to your mission and its associated important assets, as well as the tools and processes you have in place to address those threats.

This assessment is a crucial first step to starting any cybersecurity strategy, because it gets everyone on the same page about what cyber vulnerabilities, threats and technologies look like today. "What we don't want to see is people operationalizing their security based on the threats and technologies from 10 years ago, since this is a very dynamic environment." Cole said.

At the same time, you don't want to install new technologies that are incompatible with your current infrastructure. With many agencies still not working on updated operating systems, Cole said it's common to see an agency install a tool that actually can't be supported by an outdated system. Additionally, adding systems without replacing or integrating them with older tools could create a more complex, less effective security system.

Avoid these issues by executing a holistic security program assessment that examines both the threats and tools that challenge your agency's cybersecurity.

Threats

From a threat perspective, a security program assessment should consider a number of factors that define a cyberthreat, including:

- **Who is trying to compromise your organization;**
- **What they are after in your organization;**
- **Why they are trying to compromise you; and**
- **How they are trying to attack you.**

Part of that assessment might include examining similar agencies that have already assessed their threat terrain. For instance, FireEye tracks more than 16,000 threat actors across continents to determine which attacks are most likely to be coming your way in the future.

However, your assessment should go deeper to examine your own network with advanced threat-detection capabilities. Most internal assessments will reveal cyberattacks that have already infiltrated – or at least targeted – agency systems, Cole said. Use those discovered attacks to guide your understanding of threats to your organization.

"Then you can start to understand that adversary and what you need to do to create the right architecture, policies and processes to thwart those attackers," Cole said.

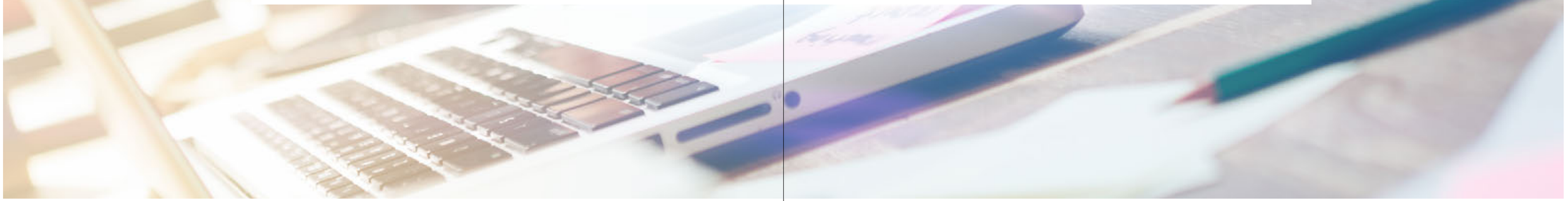
Defenses

Once you have a keen understanding of your adversary, take your assessment to the next level by considering your security mechanisms. Investigate your infrastructure and processes to consider:

- **Are your current tools and processes effectively rebuffing cyberattacks?**
- **Can those tools consume contextual threat intelligence about the adversaries?**
- **Which assets are the most exposed to threats?**
- **Are your employees capable of countering attacks in real time?**
- **What additional technologies should be acquired to counter advanced attacks?**
- **If your organization is breached, do you have a plan in place to minimize damage?**

In addition to considering what resources you have, your assessment should consider effective resource allocation. Keeping in mind which assets are most likely to be targeted by cyberattacks, leaders can determine if security tools are appropriately distributed – rather than adding layers of protection to low-priority assets that are unlikely to be targeted.

"The goal is to help agencies understand what they should be focused on, rather than trying to protect everything equally when they don't have the resources to do that," Cole said.



Support

This assessment is the first guiding step to operationalizing security in government. But especially for agencies that are behind in their cybersecurity initiatives, this holistic assessment can be a technical and procedural challenge. It requires a keen understanding of both the external threat landscape and the agency's specific environment. Moreover, the assessment should be executed without organizational biases.

For those reasons, it may be necessary to seek external support. "The one thing that is unbelievably beneficial is to actually have somebody who has no preconceived notions about your environment," said Cole. "Have someone come in and look at your environment to figure out what you're doing right and what you're doing wrong, based on best practices around the globe."

This external analysis is especially useful for organizations that have been unable to detect threats in their networks already. Companies that specialize in threat detection, like FireEye, have the tools and expertise to identify many sophisticated attacks that agencies simply aren't capable of finding with outdated systems. In fact, 47 percent of cyberattack victims learn they are breached from a third party.

Once your agency has a baseline understanding of the threats it faces, as well as the defenses it lacks to confront them, you can begin to build a strategy that operationalizes security.

The Components of Operationalized Security

Once you know what threats your organization faces and what it needs to combat them, you might be tempted to begin acquiring one-off solutions to repair specific vulnerabilities. But that's a mistake that many agencies have already made, and it's led to the complex, ineffective cyber infrastructures of many organizations today. Instead, your goal should be to create operationalized security with a suite of complementary tools and processes that integrate well together and help fill gaps in your security posture.

Cole described operationalized security as "incorporating concepts of cybersecurity across the entire environment to build a living process of security." These concepts are acutely attuned to the threats and needs found in the security program assessment. Then, procedures are established across the organizational levels to ensure that everyone is executing cybersecurity policies consistently.

That's different from many defense strategies that don't engrain security measures into the entire organization. In most cases, plans rely on IT administrators and cybersecurity personnel to cull data and alerts to recognize breaches, rather than applying tactics that maintain security constantly. Operationalized security empowers frontline users, as well as IT personnel, to safeguard the organization.

How? Cole outlined some of the fundamental components of operationalized security:

- **PRIORITIZED SAFEGUARDS.**
  By prioritizing cyber resources for targeted systems and understanding how attacks operate in your systems, you can minimize false positives, reduce alerts and focus on your most critical cyber needs.

- **INVOLVED USERS.**
  Frontline employees who understand how to identify cyberattacks like phishing emails and know what to do when they're encountered help monitor the entire organization, not just complex IT systems.

- **ENGAGED LEADERSHIP.**
  It's essential that leaders understand the role of cybersecurity in the agency's mission and relate that message to their employees. They should also include cyber in all of their process and technology decisions.

The most critical attribute of an operationalized security environment, however, is the ability to react and evolve to changing threats.

React

This is the biggest difference between operationalized security and many cyber strategies that focus on attack prevention through tactics like patching and cyber hygiene. While daily maintenance of security features is critical, those tactics fail to keep pace with evolving threats and technologies because they leverage retrospective data. Organizations need more real-time evidence to build the context necessary to anticipate attacks.

Of course, organizations should focus on preventing as many attacks as possible. Nevertheless, Cole said that a successful breach is nearly inevitable for organizations, given the volume and constant evolution of attack types. Therefore, agencies must have a contingency plan to quickly identify attacks that bypass security controls, and respond effectively. That's called breach resilience, and it's a necessary component of operationalized security.

A breach-resilient strategy requires organizations to have an integrated workflow that spans detection and visibility, as well as response and remediation. Organizations can then engage with multiple vendors and stitch together a workflow with their own capabilities through trial and error, or leverage an experienced security partner that has already assembled the elements necessary to deliver an end-to-end experience.

For instance, FireEye can create an orchestration program that defines necessary security products for a specific environment, and incorporates their operation into security strategies. FireEye's Helix solution can also help IT administrators simplify, integrate and automate security operations. This single solution reduces the complexity of your infrastructure, making it easier to detect and react to the important threats in real time and can minimize alert fatigue for analysts.

In addition to technologies, organizations will need to redesign their management processes to quickly confront attacks. That means having processes in place to ensure a swift response, even when key decision-makers are unavailable. Your remediation plan may also require having external incident-response teams on call to counter truly disruptive attacks.

Evolve

The goal of reaction and remediation is to minimize the damage done by new threats to your agency's systems. Operationalized security strategies require you to do more, however, than just react. Agency and IT leaders should also learn from those attacks and adapt their processes accordingly.

"Everything you find in your environment must be incorporated into your processes and policies for updates, so that you can continuously evolve and learn, much like the adversary does," Cole said.

Again, you'll have to consider both your technologies and the management structures that support your cyber strategies. To ensure your operational strategy can evolve quickly, you'll need to create and manage acquisition policies that can procure technologies to meet new threats as they develop.

You'll also need a partner that can help you match new threats to new technologies quickly. Vendors like FireEye can couple your agency's breach information with machine-based and adversary intelligence from other incident-response cases to truly understand the threat. In fact, FireEye's Multi-Vector Virtual Execution (MVX) engine is able to detect never-seen-before (signature-less) malicious files and URLs and quarantine them before IT administrators are even aware of an attack.

With robust threat intelligence, agencies can proactively engrain new information into their technologies and processes to create truly operationalized security.

Conclusion

Government can no longer rely on standard, one-off defenses like firewalls and antivirus software to deflect common attacks. Prevention is not enough to combat today's threats, and piecemeal infrastructures of disparate solutions only compound agencies' security challenges.

Instead, agencies must embrace the idea that cybersecurity is a core component of every policy, process and technology within an organization. Most military organizations today have accepted that cyberspace is an operational domain, and now all government agencies need to realize that we're all connected together and fighting in it whether we like it or not. Operationalized security is the only way government is going to keep up with constantly evolving cyberattacks, despite fewer resources and personnel to get the job done. That will require an ongoing commitment to assess the threat landscape, incorporate intelligence into holistic strategies and adjust in the face of new threats.

About FireEye

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 5,600 customers across 67 countries, including more than 40 percent of the Forbes Global 2000.

About GovLoop

GovLoop's mission is to "connect government to improve government." We aim to inspire public-sector professionals by serving as the knowledge network for government. GovLoop connects more than 250,000 members, fostering cross-government collaboration, solving common problems and advancing government careers. GovLoop is headquartered in Washington, D.C., with a team of dedicated professionals who share a commitment to connect and improve government.

For more information about this report, please reach out to info@govloop.com.

1152 15th Street NW, Suite 800
Washington, DC 20005
Phone: (202) 407-7421 | Fax: (202) 407-7501
www.govloop.com | @GovLoop