EMPOWERING AGENCY ANALYSTS TO MINIMIZE RISKS

As public information is increasingly digitized, cyberthreats and breaches have the potential to cause catastrophic damage. As society has become increasingly reliant on digital communications and transactions, protecting citizen data from data breaches, intrusions or insider threats is now of the most paramount concern.

With this in mind, cybersecurity mandates and security compliance has become a top priority for public agencies. For a more in-depth perspective, we spoke with Travis Rosiek, Chief Solution Strategist for Global Government at FireEye.

Rosiek notes that compliance to cyber regulations and norms is not enough. "What I've seen in my experience is compliance doesn't mean secure," said Rosiek. He states it is more important for agencies to focus on security, such as detecting and minimizing the threat and impact of cyber attacks. Compliance should be a result of these efforts, but not the sole objective.

When it comes to helping organizations remain secure, FireEye protects agencies from cyber threats with its custom-built security platforms that are specifically designed for real-time malware analysis. "[The Multi-Vector Virtual Execution (MVX) engine] is designed with such high-performance and efficacy that we can actually generate intelligence on premise that can be used to minimize the impact of a current threat without user interaction," explains Rosiek.

FireEye helps minimize risks by empowering agency analysts and security teams, giving them actionable information with rich context around suspicious activity. With the sophistication of the next generation of cyber attacks, the automatic execution of pre-approved security measures helps improve consistency and early detection. This is especially important given that a 2013 Mandiant report found the median time from an organization data breach to detection was 229 days. What's more, 67 percent of these organizations only learned of the breach via third party notifications and 100% had Antivirus up to date.

Additionally, it is critical for organizations to stay current on the latest cybersecurity strategies, advises Rosiek. Agencies need to promote continual learning and be aware of new vulnerabilities. Employee training and a sound security infrastructure are crucial to this effort.

"By understanding the capabilities of your adversaries you can better posture yourself – whether it be personally for training (i.e. how attacks works) or for your organization's security infrastructure – and this will mitigate some threats," says Rosiek.

And it doesn't matter if you're not a high-profile organization or in an IT-related field. "Most people don't think that their information is important," Rosiek notes. "But to an adversary or competition or somebody else, it's invaluable." Since cybersecurity programs impact everyone, it is important to clearly communicate with all employees, provide relevant context, and avoid intimidating technical jargon.

On an everyday basis, organizations face the daunting task of protecting their information networks. Given Rosiek's experience working with public sector organizations, he provided what he views as the top five current cyber challenges:

1. **Acquisition models** – The majority of the public sector's IT/cyber defense acquisition models are lacking. The adoption of technology including cloud and mobile applications are creating new concerns regarding privacy and security. Keeping up with this rapidly evolving landscape can prove to be a significant task.
2. **Cyber Workforce** – Low retention rates and shortages of the cyber workforce in the U.S. impede progress towards sustainable and secure organizations. To address this concern, FireEye launched initiatives with STEM students, aiming to get young people more interested in this high-demand field.
3. **Cyber Legislation** – Contention on the Hill regarding cyber security laws slows down or prevents progress. For the legislation that is out there, there are often significant gaps in the policy or implementation.
4. **Legal Constraints** – Globally Cyber defenders have many legal constraints they must navigate. "Adversaries know what these legal constraints are and they use them to their advantage," says Rosiek.
5. **Cyber Mindset** – The importance of being compliant versus being thoroughly secure. Organizations should understand that it is essentially inevitable that they will be breached at some point. Thus, preparation and planning are critical to reduce cyber risks and minimize potential damage.

Although these are the challenges that agencies face today, it's important to remember that the threat landscape is constantly changing and evolving. As tools grow in sophistication, so do the threats facing agencies. Due to this, organizations must be sure they have created a culture of cybersecurity, and staying current with the latest threat detection and mitigation strategies.

Today, public agencies must navigate a digital landscape full of increasingly complex cyber threats. However, with better awareness and training, and the help of cybersecurity vendors like FireEye, such challenges can be faced with confidence.