THE ALS GROUP

Managing Risk to Influence Successful Outcomes

Preventing Swatting

Authored by
Albert L. Sica

Preventing Swatting: How to Defend Against Cyber Attacks

At The ALS Group, we are acutely aware of the evolving threats in the digital landscape, and swatting represents a particularly malicious form of cyber-attack with real-world implications. As a risk advisory firm, our mission is to illuminate the dangers of such activities and provide strategic risk mitigation strategies to safeguard businesses and individuals alike.

Understanding Swatting: A High-Risk Threat

Swatting is a dangerous and illegal act where perpetrators make hoax calls to emergency services, fabricating a critical situation that leads to the deployment of armed law enforcement, such as SWAT teams, to an unsuspecting target's location. This malicious act can result in severe consequences, including injury, wrongful death, property damage, and significant emotional distress, not to mention the considerable waste of public safety resources and the inherent risk it poses to law enforcement personnel.

The Fred Hutchinson Cancer Center in Seattle experienced a swatting attack in November 2023 when threat actors stole medical records and wanted to heighten the stakes by menacing the center's patients. As a result, the FBI and Seattle police were notified, and the FBI investigated said threats.

Integris Health in Oklahoma also endured a cyber-incident when some patients started receiving emails from threat actors with demands, then threatening to sell their personal information if those demands were not met.

There are several risk factors to consider when it comes to swatting. These include the immediate danger to physical safety, as well as the potential for long-term reputational damage, legal consequences, and financial liabilities. Ways to prevent swatting include:

1. Educational Awareness: Educating your staff is a critical component of Cyber security. It's important to understand not only swatting and the various techniques involved, such as caller ID spoofing, hacking, and social engineering but also other methods of potential cyber-attacks. This knowledge can help individuals and businesses identify potential vulnerabilities. It's a good idea to have regular training sessions for staff and community members. This will help them learn how to recognize and respond to potential swatting attempts. It's important to emphasize the significance of cybersecurity awareness in preventing such incidents.

2. Preventative Measures: It's important to take privacy seriously to prevent personal and organizational information leaks that could potentially result in swatting incidents. We recommend adopting a comprehensive approach to safeguarding your privacy. We make sure to regularly check your online presence to protect sensitive information from being publicly accessible. We also recommend the use of cyber-encryption techniques for secure communications and the implementation of two-factor authentication for all our digital platforms. Understanding digital footprints can greatly decrease the chances of becoming a target.

3. Enhanced Security Infrastructure: Using advanced security technologies that can detect and respond to threats can make a significant difference in preventing swatting incidents. There are various solutions available to help protect your network from malicious activities. Endpoint Protection Software, Firewalls, anti-spoofing software, and network monitoring tools are some examples of these solutions. They can effectively detect and block any potential threats. Using a Virtual Private Network (VPN) can help individuals mask their IP address and make it harder for perpetrators to determine their location.

4. Law Enforcement Collaboration: Working together with local law enforcement is crucial. Engaging with law enforcement to discuss swatting and risk response strategies can be beneficial for businesses and high-risk individuals. It can help ensure that emergency responses are more nuanced and effective. By signing up for a law enforcement opt-in system, if it's offered in your area, you can make sure that officers are alerted in advance if a call might be a prank. This can help to defuse the situation before it gets worse.

5. Community Engagement: Developing a culture that prioritizes risk awareness can significantly improve overall security for both organizations and communities. It's important to encourage the reporting of any threats or suspicious behavior and share knowledge on how to avoid falling victim to swatting. Creating platforms where people can freely exchange their experiences and strategies can be a powerful way to help individuals and communities safeguard themselves, and others from these harmful incidents.

6. Legal Preparedness: It's important to be prepared for the legal consequences that can arise from swatting incidents. It's vital to have a good grasp of the possibility of criminal charges for those responsible and the legal options for victims. Organizations need to have a well-prepared legal action plan for cyber-security. This includes having protocols in place for collaborating with law enforcement to track and prosecute offenders, as well as strategies for effectively handling any potential public relations issues that may arise from swatting incidents.

Dealing with swatting requires a proactive and well-informed approach. At The ALS Group, we believe in taking a comprehensive approach to risk management. By combining technological solutions, educational initiatives, and legal strategies, we aim to strengthen defenses against potential threats.

Understanding the importance of education, implementing strong security measures, and working closely with law enforcement are crucial in reducing the risks associated with swatting. By implementing these strategies, we can ensure the safety of our communities, conserve public safety resources, and discourage individuals with malicious intent from taking advantage of vulnerabilities in both our digital and physical surroundings.

If you have any questions on cyber risk or security or want to review your company's cyber threats, please contact Jon Edwards, Managing Director, at 732-395-4281 or jedwards@thealsgroup.com.