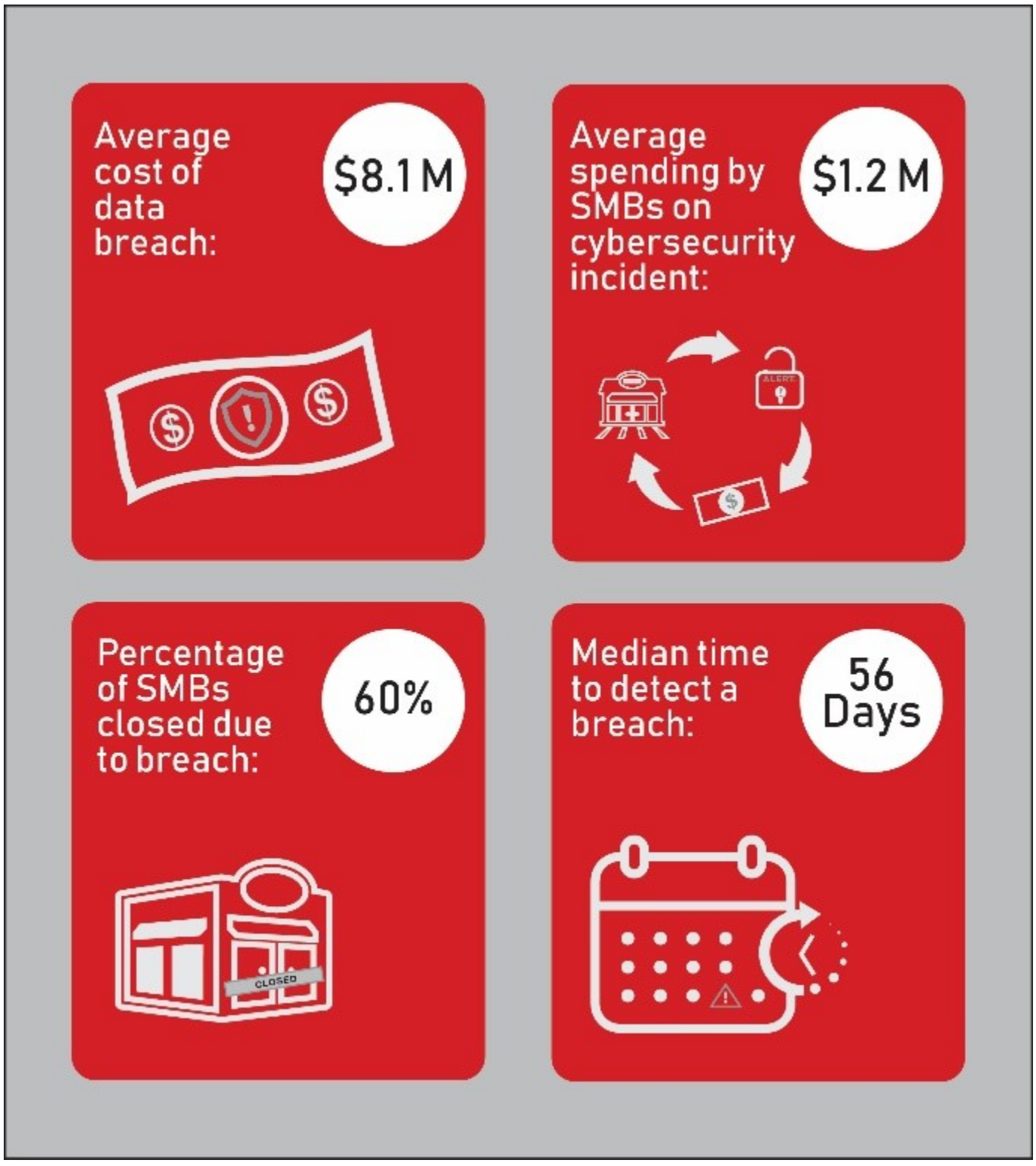
Offensive vs. Defensive Cybersecurity

February 2, 2021

Amidst the COVID-19 pandemic and subsequent stay-at-home order, the global market has become increasingly reliant on Internet connectivity and, most importantly, their IT infrastructure, to operate remotely. However, cyber criminals and Advanced Persistent Threat (APT) groups have taken notice of this, and seek to exploit organizations that are not adequately prepared for a cyber attack. In fact, experts estimate that over 300,000 new variants of malware and potential unwanted programs are developed daily.

For small and medium sized businesses (SMBs) in the United States, the average cost of a data breach is $2.2 million. Often these businesses are forced to close due to complications arising from a breach. In this article, learn more about how you can mitigate the risk of cyber attacks to your SMB through a mix of offensive and defensive cybersecurity postures.

Offensive vs. Defensive Cybersecurity



Today, most SMBs cyber security practices are based on defensive cyber security principles. This approach focuses on patch management, Security Information and Event Management (SIEM) implementation, log management and perimeter hardening. However, while defensive cyber security measures are essential, implementing offensive cybersecurity measures is necessary to effectively protect

your SMB from cyber criminals.

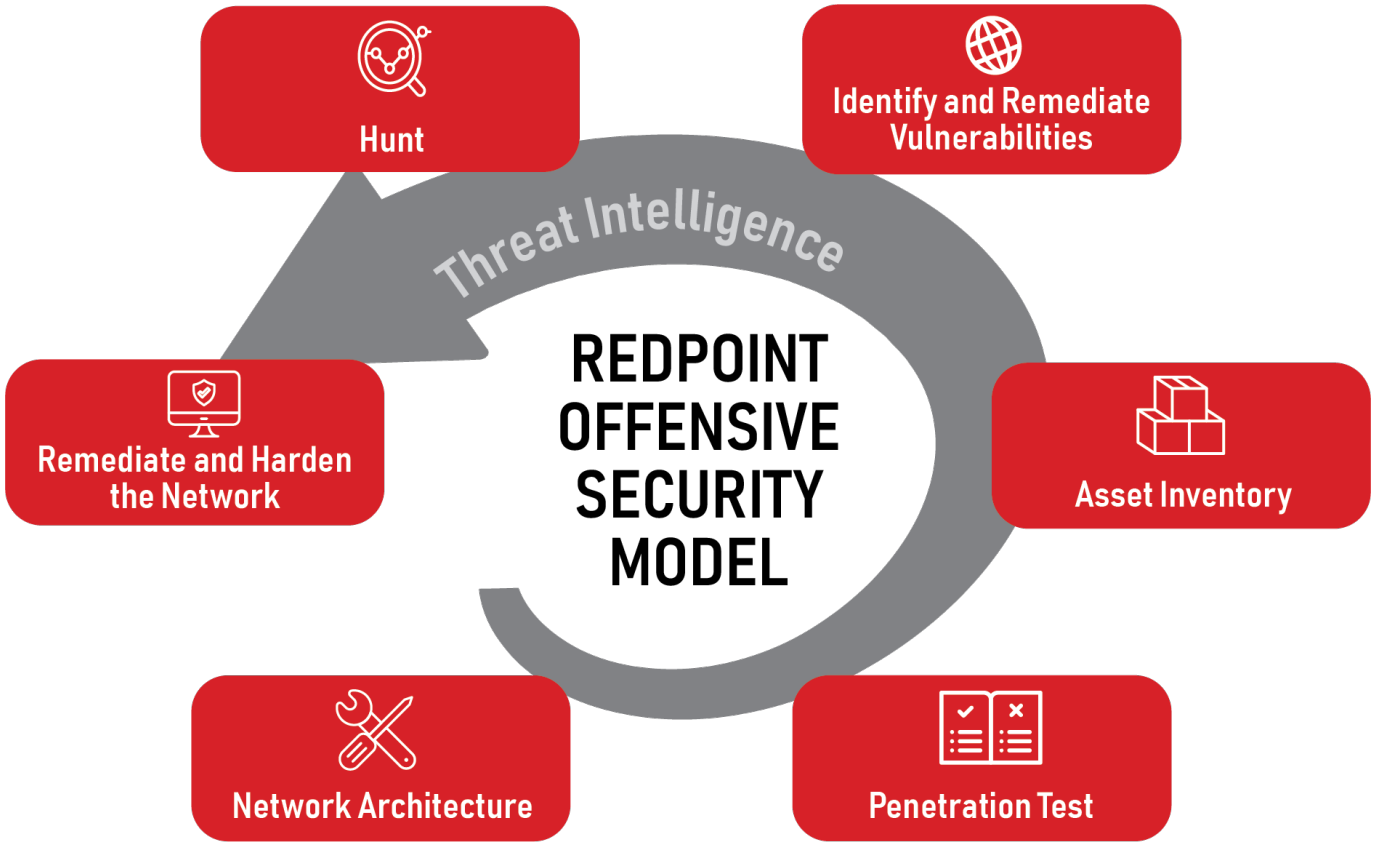
Offensive cyber security strategies preemptively identify vulnerabilities and security weaknesses before an attacker exploits them. Offensive cyber security teams actively test the network's defenses and provide valuable insights into an organization's cyber security posture. Two of the most effective offensive cyber security approaches are Threat Hunting and Penetration Testing (Pentesting).

Pentesting identifies vulnerabilities on an organization's network. Threat Hunters can then actively hunt for an attacker's presence on an organization's network by exploiting these vulnerabilities and using known attacker tactics, techniques and procedures. Effective regular Pentesting and Threat Hunting paired with a robust defensive strategy helps to mitigate risk and reduce potential financial loss due to a cyber attack. Organizations that combine these two tactics can efficiently identify attackers on their network, significantly reducing the overall costs for remediation and the potential costs associated with a breach.

Redpoint's Threat Mitigation Group

Redpoint's Threat Mitigation Group keeps your organization secure through a unique approach to target, pursue, and eliminate threats on your network – we "Hunt the Hunter". Comprised of experts in both offensive and defensive cyber security strategies, Redpoint Cybersecurity can partner with you to create a robust cyber security program for your SMB and curate industry-specific threat intelligence to provide insight into the cyber threat landscape.

Our approach is to align security with business strategy. We take actionable steps to help our clients mitigate their risk by combining Threat Hunting and Pentesting to secure your network. Redpoint's solutions will align with executive- and board-level desired outcomes to mitigate risk and reduce exposure, and our human-led, technology-enabled ethos gives us the ability to tailor cutting edge technology to your organizational objectives.



For more information, please contact Tab Bradshaw at tab@redpointcyber.com.