Photo: Josh Edge, GCI

Presented by: GCI

In partnership with: CISCO Partner | CI Security | Northpoint A GCI COMPANY

Cyber Security Experts Address Latest Trends in Today's Evolving Global Digital Realm

Crypojacking, whaling, cyber-attacks and RDP comprise key topics at cybersecurity breakfast hosted by GCI and Northpoint in partnership with British-American Business

(SEATTLE, Oct. 17, 2018) From cryptojacking to whaling, cyber-attacks vary widely in scope and sophistication. Preventing and heading off these threats requires a high degree of vigilance and expertise. A panel discussion co-hosted by Northpoint, a GCI company, and the Pacific Northwest chapter of British-American Business Connections covered the latest cybersecurity trends in an ever-evolving digital realm.

With nearly 50 people in attendance, experts from Northpoint, GCI, HSBC Bank and CI Security gathered in downtown Seattle to discuss the most-critical cybersecurity issues faced by businesses and the processes necessary to protect their networks, information, people and profits. Sponsors of the event included GCI, Northpoint, Cisco Partners, and CI Security

"We were pleased to have the opportunity to join with our BABC members, GCI and Northpoint, to present a deeper dive into critical reasons companies should be examining internal processes and procedures beyond just their customer facing systems," said Catherine Filippini, executive director for British-American Business Connections. "While companies or their employees many be aware of issues at a surface level, the chance to understand more specific scenarios that can easily impact business operations is critical to preventing worst case security breaches."

"The threat landscape is constantly changing and is incredibly difficult to stay on top of," said John Barnhardt, vice president, GCI Business Product Development. "This year, the predominant new thing coming to the forefront is cryptojacking, where people take over machines on your network to mine for cryptocurrency."

Among the plethora of other digital threats facing businesses and network system managers is the rise of threats through Remote Desktop Protocol (RDP), which provides a user with a graphical interface to connect to another computer over a network connection. Through RDP, hackers can gain access to vast amounts of confidential information and critical systems, compromising networks and potentially hamstringing a company.

“You have to be vigilant over time, there’s no silver bullet,” said Jeff Ridgeley, cybersecurity practice manager, Northpoint. “Protecting yourself from these kinds of intrusions requires some basic hygiene inside networks and in the cloud – like managing and controlling access to privileged accounts and turning on multi-factor authentication.”

Multi-factor authentication is a method for confirming a user’s claimed identity through two or more levels of authentication that can include anything from a card swipe and PIN to one-time passwords and biometric scans. Without these types of precautions, businesses leave their networks, information and funds vulnerable to attacks, hacks and scams.

Attempts to falsely gain access to privileged information and accounts are not limited to high-tech, brute force attacks. Some are more rudimentary, but just as effective, like phishing attempts though the mimicking of an executive’s email address, or even by going analogue and submitting an altered and forged physical invoice in an attempt to fool those with the keys to spending accounts, according to Siva Ram, the head of Business Security & Fraud Risk for HSBC Bank. That is why it’s important to have what’s referred to in cybersecurity circles as “defense-in-depth.”

“Having a single line of defense, like a firewall, just won’t do; there needs to be progressive layers of security, something in place to stop them at the next layer,” said Barnhardt. “An effective security plan is like a three-legged stool; you need a system, processes and people. It needs to be holistic and all of the elements need to work together.”

Whether you’re securing personal employee data, protected HIPPA information, working on a government contract or anything in between, security has become a competitive differentiator in business, according to Michael Hamilton, co-founder of CI Security. The need to protect information from cyber-intrusions is vital and the expertise necessary to implement a plan is more complex than ever. Keeping up with a constantly evolving threat landscape is a task many companies are not necessarily equipped to do on their own.

“Some larger companies have the resources to handle cybersecurity issues internally, but with many businesses, maintaining an in-house team isn’t feasible,” said Ridgeley. “Instead, these businesses can seek out managed service providers and often buy services incrementally, depending on the company’s needs.”

Managed service providers, like Northpoint and CI Security, have the ability to support businesses through a variety of security solutions. With managed detection and response capabilities, experts can monitor your environment, investigate alerts to determine whether they are a false-positive or a potential threat, and respond with the appropriate actions to mitigate or eliminate the threat.

Experts can also periodically screen systems to quickly identify vulnerabilities and test network weaknesses by emulating hacker tools, techniques and tactics to uncover gaps in your IT environment. Cybersecurity teams dedicate their careers to staying on top of the latest cybersecurity trends and work to protect companies’ information and assets, reduce information overload, eliminate repetitive and manual maintenance, and develop unique security solutions to meet customers’ needs.

To connect with Northpoint, visit their website at https://northpoint.gci.com. To learn more about British-American Business Connections visit www.babcpnw.org.

Author: Josh Edge, GCI

###