Northpoint
A GCI COMPANY

BABC 2018 CYBER SECURITY BREAKFAST
OCT. 17, 2018

Schedule

7:30 a.m. — 8 a.m.	Registration, Breakfast, and Networking
8 a.m. — 9 a.m.	Panel Discussion
9 a.m. — 9:15 a.m.	Q&A
9:15 a.m. — 9:30 a.m.	Networking and Adjourn

SPEAKERS

John Barnhardt
VP Business Product Development, GCI

David Fowler
VP Strategic Services & Privacy Compliance, Fishbowl

Michael Hamilton, CISSP
Former Chief Information Security Officer, City of Seattle

Jeff Ridgeley
Cyber Security Architect, Northpoint

Siva Ram
Head, Business Security & Fraud Risk, GLCM Digital Channels, HSBC

Help Reduce Your Risk for Remote Desktop (RDP) Attacks

The FBI, in partnership with the Department of Homeland Security, recommends the following in regard to improving RDP security:

- Audit your network for systems using RDP for remote communication; install available patches, or disable service if it is not needed.
- Verify that all cloud-based virtual machine instances with a public IP do not have open RDP ports, specifically port 3389, without a valid business reason. Place any system with an open RDP port behind a firewall and require users to use a virtual private network (VPN) to access it.
- Enable strong passwords and account lockout policies to defend against brute-force attacks.
- Apply two-factor authentication, where possible.
- Apply system and software updates regularly.
- Maintain a good back-up strategy.
- Enable logging and ensure mechanisms capture RDP logins. Keep logs for a minimum of 90 days and review them regularly to detect intrusion attempts.
- When creating cloud-based virtual machines, adhere to the cloud provider's best practices for remote access.
- Require third parties with RDP access to follow internal policies on remote access.
- Minimize network exposure for all control system devices. Where possible, critical devices should not have RDP enabled.
- Regulate and limit external-to-internal RDP connections; when required, use secure methods, such as VPNs.

Northpoint
A GCI COMPANY

Managed Security Solutions

Managed Detection and Response

Monitor your environment, investigate alerts to determine whether they are a false-positive or a potential threat, and be advised with the appropriate actions to mitigate or eliminate the threat, with our Managed Detection and Response (MDR) solution. This comprehensive service includes the hardware, software, and services necessary to improve your security posture and includes 24/7/365 monitoring and support from a security operations center (SOC), satisfying many audit, compliance, and security monitoring requirements.

Penetration Testing

Identify ways an attacker may compromise your network by emulating hacker tools, techniques, and tactics to uncover gaps, holes, and vulnerabilities in your IT environment. This service satisfies all major compliance standards and findings are summarized to include recommendations to remediate observed weaknesses.

Vulnerability Scanning

Schedule network scans to quickly identify vulnerabilities on a one-time or recurring basis, at whatever interval you prescribe.

vCISO Services

Experience CISO-level support for a fixed period of time, creating an affordable option to access CISO expertise.

For a complete listing of Northpoint's cybersecurity capabilities, visit northpoint.gci.com/cybersecurity, or call (206) 708-7177.

Northpoint
A GCI COMPANY

Northpoint
northpoint.gci.com
16300 Christensen Rd.
Suite 350
Tukwila, WA 98188
(206) 708-7177

CI Security

CI Security:
CI Security
https://ci.security
245 4th St., Suite 405
Bremerton, WA 98989
+1 206 687 9100