Planning 3rd Party Access to Sensitive Networks

SECURITY AND CONVENIENCE ARE AT OPPOSITE ENDS OF THE SPECTRUM. PLAN WISELY!

Design Criteria

- Every environment is different, keep your IT/OT staff involved in evaluating risks throughout the process.
- Before you set your ground-rules for any 3rd Party connections, ask the big six qualifiers:
  - "Who, What, When, Where, How, and Why?"
- Use this information to help build successful RFPs and bid packages.
- Ensure that you are including cybersecurity in the bid evaluation processes and also in the executed contracts.

- Everybody remembers Fazio Mechanical, right?

WHO?

- Is this an individual or company that will be provided with remote access?
- If a company, how does that entity handle employee vetting and turnover?
- Does this entity have an established culture of cybersecurity?
  - Do they run appropriate anti-virus/anti-malware on their systems?
  - Do their applications and programmers take security into account?
  - Do they demonstrate proper care when transferring data during negotiations?

WHAT?

- What target device(s) will be receiving remote connections?
  - Are the target(s) software or hardware based?
- Does the target include control functions, or just monitoring?

- What device(s) will be used to initiate the connections?
  - Work PCs? Laptops? Mobile devices? Home PCs?
  - Are those devices secured? Updated/Patched regularly?
  - Are the networks these devices use properly firewalled/secured?

WHEN?

- When would 3rd parties be connecting to your devices?
- Are there times that you wouldn't want them connected?
- Are there time-zone constraints for the connections?
- Would the timing of the remote connections interrupt other key functions like backups or maintenance?

- Will the connection be always-on (like a site-to-site VPN), or session based (such as RDP)?
- Will you be able to see who is using the resources when they are connected?

WHERE?

- Where will connections to the resources be initiated from?
  - Static locations (e.g. a business office)?
  - Transient locations, like mobile devices or laptops?
  - Via a bridge connection to a user within your organization?
  - Foreign countries allowed?
- What part of your network will the connection terminate into?
  - Can the initiator see other sensitive systems in that same space?
  - Is there adequate bandwidth to support the additional connection(s)?

HOW?

- Will you use a VPN, RDP, or a remote session to an internal technician who bridges to the resource? Or maybe some other software to allow connections?

- Will you use Multi-Factor Authentication for session based connections?
  - If so, will it be based upon hard tokens, soft tokens, SMS, or other?
  - How will MFA tokens be distributed?
  - How will lost tokens or mobile devices be handled?

WHY?

- It is important to ask why the connection is important to the 3rd party.
  - The best way to not have issues with remote connections is to simply not use them.
  - Maybe their needs can be solved another way?
  - If used for log collection and performance monitoring (read-only), your security posture may be different than if the connection can be used for tuning and controls (change-enabled).
- What value does your organization get from the remote connection?