# Next Level of Security Compliance

## Creating Operational Excellence and Mission Assurance

October 26, 2017

**Bill Johnson** - TDI Technologies
**Patrick Miller** - Archer Security Group

tdi
ConsoleWorks
Cybersecurity Operations Platform

ARCHER
SECURITY GROUP

# Thank You for Attending!

- Q&A will be at the end of the webinar
- Send your questions at any time during the presentation and we will queue them up to be answered

**How to Ask Questions**

1. Click on the Questions and Answers icon to submit a question to all panelists
2. Type your question in the box and click Send
3. Click on the Chat to send comment to "All Panelists" or "Everyone"
4. Type your comment, question, or URL and hit <Enter>
5. Raise Hand to get Host's attention



12042 SE Sunnyside Road #292 Clackamas OR 97015 | 800-805-7411
www.archerenergysolutions.com | info@archerenergy.solutions

# Introductions

**Presenters**

## Bill Johnson
President & CEO
TDi Technologies
www.tditechnologies.com

## Patrick C Miller
Managing Partner
Archer Security Group
www.archersecuritygroup.com



12042 SE Sunnyside Road #292 Clackamas OR 97015 | 800-805-7411
www.archerenergysolutions.com | info@archerenergy.solutions

# Today's Webinar Format




12042 SE Sunnyside Road #292 Clackamas OR 97015 | 800-805-7411
www.archerenergysolutions.com | info@archerenergy.solutions

# Goal: Mission Assurance

- What is it?

*Strategic execution of the business goal despite tactical operational inconsistencies*

- How is it different than… ?
  - Security
  - Compliance
  - Resilience




12042 SE Sunnyside Road #292 Clackamas OR 97015 | 800-805-7411
www.archerenergysolutions.com | info@archerenergy.solutions

# Goal: Operational Excellence

- Do more with less
- Proactive vs. reactive
- Get back to your "day job"
- Measuring for continuous improvement



12042 SE Sunnyside Road #292 Clackamas OR 97015 | 800-805-7411
www.archerenergysolutions.com | info@archerenergy.solutions

# Goal: Security AND Compliance

- You can be secure and noncompliant
- You can be compliant and not secure
- You will do some things just for compliance
- You will do some things just for security
- You CAN do both in many areas, but this is the hardest (and most valuable) path…


12042 SE Sunnyside Road #292 Clackamas OR 97015 | 800-805-7411
www.archerenergysolutions.com | info@archerenergy.solutions

# Challenges: People

- Not enough of them
- Skillsets
- Budget
- Hanlon's Razor
- Culture



12042 SE Sunnyside Road #292 Clackamas OR 97015 | 800-805-7411
www.archerenergysolutions.com | info@archerenergy.solutions

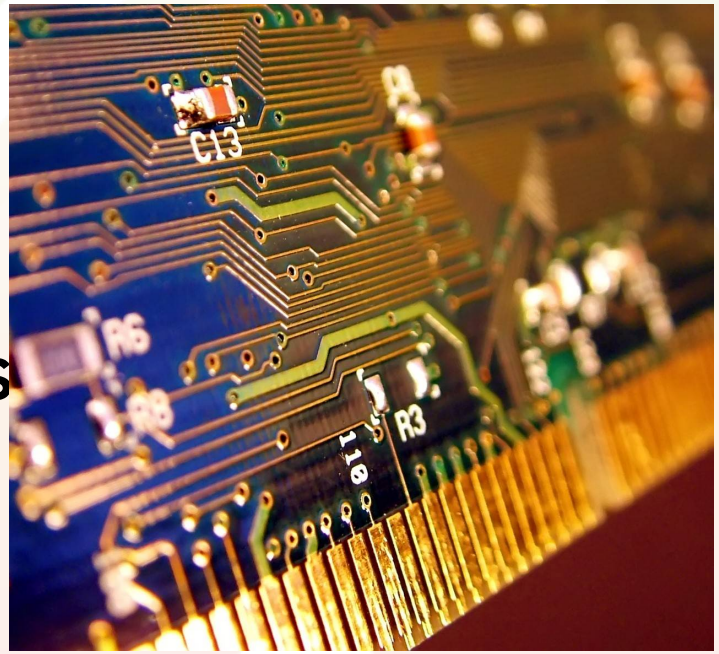
# Challenges: Process

- You know what you're doing. Why do you have to write it down?
- Policy, procedure or process?
- Reflecting reality
- Manual vs automated


12042 SE Sunnyside Road #292 Clackamas OR 97015 | 800-805-7411
www.archerenergysolutions.com | info@archerenergy.solutions

# Challenges: Technology

- Too much vs. too little
- Tool overlap
- Complexity
- Set and forget
- Integration
- Sacred cows and egos
- OT and IT…






12042 SE Sunnyside Road #292 Clackamas OR 97015 | 800-805-7411
www.archerenergysolutions.com | info@archerenergy.solutions

# Challenges: OT, IT and just T

| IT | OT / ICS |
|---|---|
| Protect data | Availability and safety |
| Protection from the Internet | No internet access at many plants |
| Modern systems and OS | Some that are 30 years old and no longer supported |
| Dynamic (people and devices come and go frequently) | Static environments (people and devices are around for a long time) |
| Extensive automation of tools | High level of control with manual processes |
| Standard communication protocols | Proprietary protocols |
| Patches freely installed (relatively quickly) | Rigorously tested by vendor for compatibility (slow) |
| Configuration changes occur frequently | Highly controlled for reliability & safety reasons |


12042 SE Sunnyside Road #292 Clackamas OR 97015 | 800-805-7411
www.archerenergysolutions.com | info@archerenergy.solutions

# Where Do You Start?

- Get management buy-in: resilience, cost savings
- Prioritize with a risk analysis
- Follow up with a gap analysis, merge both
  - People, Process, Technology
- Compile all current security/compliance metrics
- Be realistic about change; expect roadblocks
- Target high-value areas, but don't forget the low-hanging fruit

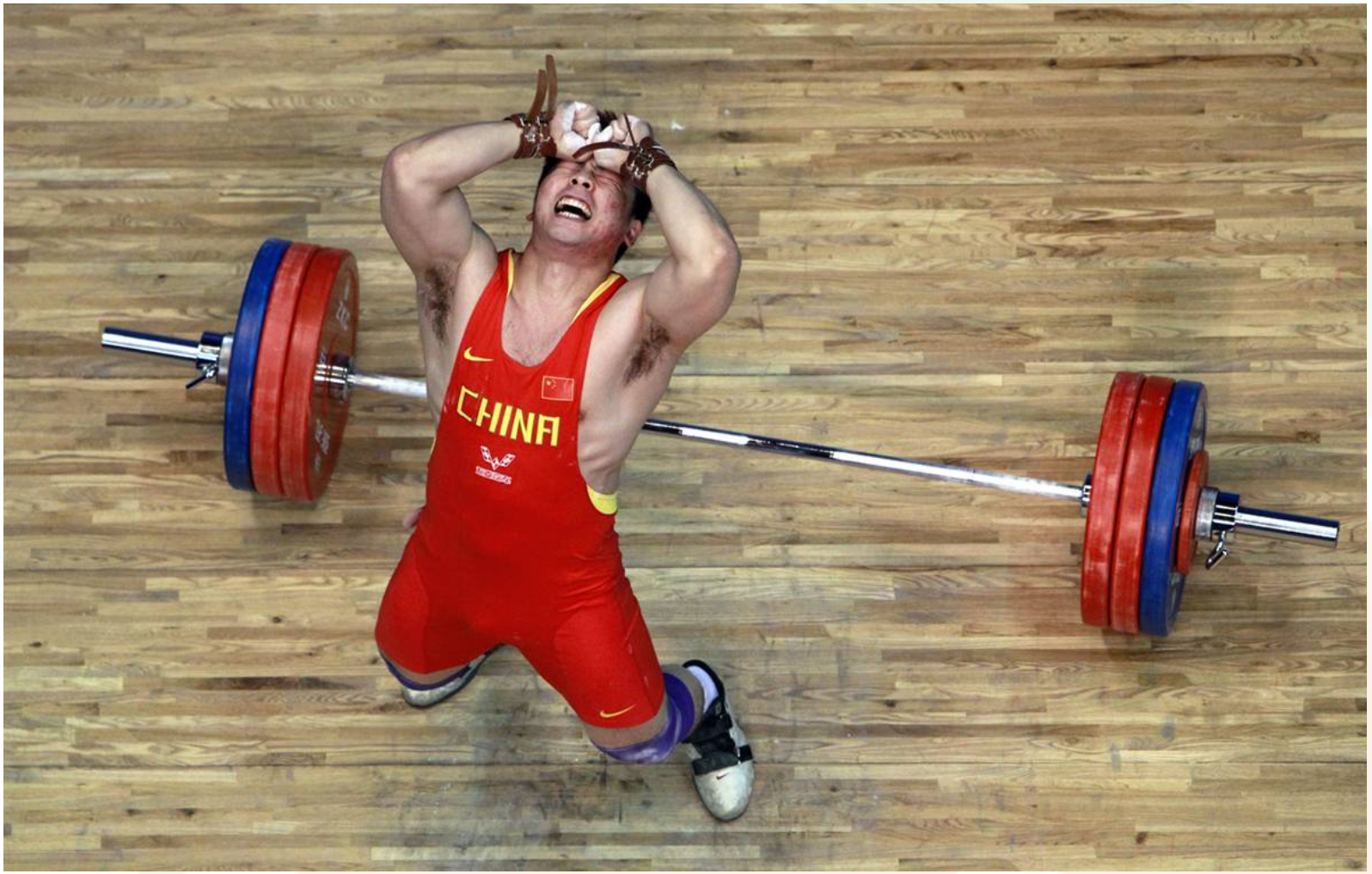

12042 SE Sunnyside Road #292 Clackamas OR 97015 | 800-805-7411
www.archerenergysolutions.com | info@archerenergy.solutions

# Baby Steps

- Build your technology blueprint/inventory
- Use analyses to frame approach
- Look for process revisions, with an eye toward controls and [targeted] automation
- Begin revision of process and automation in conjunction
- Lather, rinse, repeat


12042 SE Sunnyside Road #292 Clackamas OR 97015 | 800-805-7411
www.archerenergysolutions.com | info@archerenergy.solutions

# Change Is Hard






12042 SE Sunnyside Road #292 Clackamas OR 97015 | 800-805-7411
www.archerenergysolutions.com | info@archerenergy.solutions

# Build a Defendable Environment

- Segment critical systems into enclaves
- Minimize dependencies on other segments
- Insert network monitoring points
- Don’t forget that you still have to manage it



12042 SE Sunnyside Road #292 Clackamas OR 97015 | 800-805-7411
www.archerenergysolutions.com | info@archerenergy.solutions

# Reduce Your Surface Area

- Eliminate tool overlap, waste
- Establish a technology blueprint
- Standardize
- Kill any service that isn't required
- Remove anything noncritical from critical network segments


12042 SE Sunnyside Road #292 Clackamas OR 97015 | 800-805-7411
www.archerenergysolutions.com | info@archerenergy.solutions

# Phase Out Fragile Systems

- Homogenize builds as much as possible
- Remove hard to manage snowflakes
- Start planning for ICS upgrades
- Shrink footprint of legacy equipment



12042 SE Sunnyside Road #292 Clackamas OR 97015 | 800-805-7411
www.archerenergysolutions.com | info@archerenergy.solutions

# Get Access Under Control

- Fewer access points to manage
- Fewer people to manage
- Multifactor authentication for remote access


12042 SE Sunnyside Road #292 Clackamas OR 97015 | 800-805-7411
www.archerenergysolutions.com | info@archerenergy.solutions

# The Patching Problem

- 90% of the "problem"
- Can range from hard to very hard
- Some vendors are getting better
- Will eventually become a diligence argument


12042 SE Sunnyside Road #292 Clackamas OR 97015 | 800-805-7411
www.archerenergysolutions.com | info@archerenergy.solutions

# Change and Config Management

- Simply put, best bang for the buck
- Compliance bonus points
- Hanlon's Razor repellent
- Faster recoverability and root cause analysis
- Great for metrics


12042 SE Sunnyside Road #292 Clackamas OR 97015 | 800-805-7411
www.archerenergysolutions.com | info@archerenergy.solutions

# Monitor Everything

- If it produces a log, get it into a SIEM
- If not, monitor the network
- Disk space is inexpensive
- Security telemetry = operational telemetry
- Data is the new oil
- Diligence and insurance bonus points


12042 SE Sunnyside Road #292 Clackamas OR 97015 | 800-805-7411
www.archerenergysolutions.com | info@archerenergy.solutions

# Get The People Onboard

- Training and awareness – at all levels
- Use security metrics, less FUD
- Accountability, diligence and liability


12042 SE Sunnyside Road #292 Clackamas OR 97015 | 800-805-7411
www.archerenergysolutions.com | info@archerenergy.solutions

# Don’t Start From Scratch

- Understand controls
- Capability Maturity Models
- Frameworks


12042 SE Sunnyside Road #292 Clackamas OR 97015 | 800-805-7411
www.archerenergysolutions.com | info@archerenergy.solutions

# Buy Smart

- Procurement language
- Supply chain risks/compliance
- If it doesn't fit your technology blueprint, keep looking
- Request pilots, bake-offs


12042 SE Sunnyside Road #292 Clackamas OR 97015 | 800-805-7411
www.archerenergysolutions.com | info@archerenergy.solutions

# Get Help

- You can't smell your own breath
- Negotiate for professional services, regular maintenance
- Integrators
- Outsourcing and Cloud


12042 SE Sunnyside Road #292 Clackamas OR 97015 | 800-805-7411
www.archerenergysolutions.com | info@archerenergy.solutions

# Conclusion

- Your goal isn't security or compliance but they can support mission assurance
- Operational excellence is a path, not a place
- Be realistic about what to do and when
- Focus on people, process and technology
- All of this is good for business and will make you more resilient and profitable


12042 SE Sunnyside Road #292 Clackamas OR 97015 | 800-805-7411
www.archerenergysolutions.com | info@archerenergy.solutions

# Q&A



12042 SE Sunnyside Road #292 Clackamas OR 97015 | 800-805-7411
www.archerenergysolutions.com | info@archerenergy.solutions

# Thank you very much!

Bill Johnson, President and CIO
TDI Technologies, Inc.
bill.johnson@tditechnologies.com

Patrick C Miller, Managing Partner
Archer Security Group
p.miller@archersecuritygroup.com