



Advanced Solutions

## Cyber Security and the New Frontier: Lessons Learned

POWERED BY  
**MATRIKON**

**Honeywell**

# AGENDA

- Introduction to Advanced Solutions' Industrial Cyber Security
- Industrial cyber security challenges
- North America 1<sup>st</sup> Regulated Industry - Power
- Long-term strategy
- Q&A

# INDUSTRIAL CYBER SECURITY

Unique Combination of:

- Control system experience
- Cyber security knowledge
- Deep understanding of process control environments

Provide various services to our clients including:

- Security vulnerability assessments, gap analysis and readiness audits
- Design and implement technical solutions (i.e. DMZ networks, virtual environments, patch management)
- Assist in establishing and maintaining security programs for corporate & regulatory compliance
- Trusted advisor for our clients

POWERED BY  
**MATRIKON**

**Experience**

12+ years experience providing industrial strength security solutions

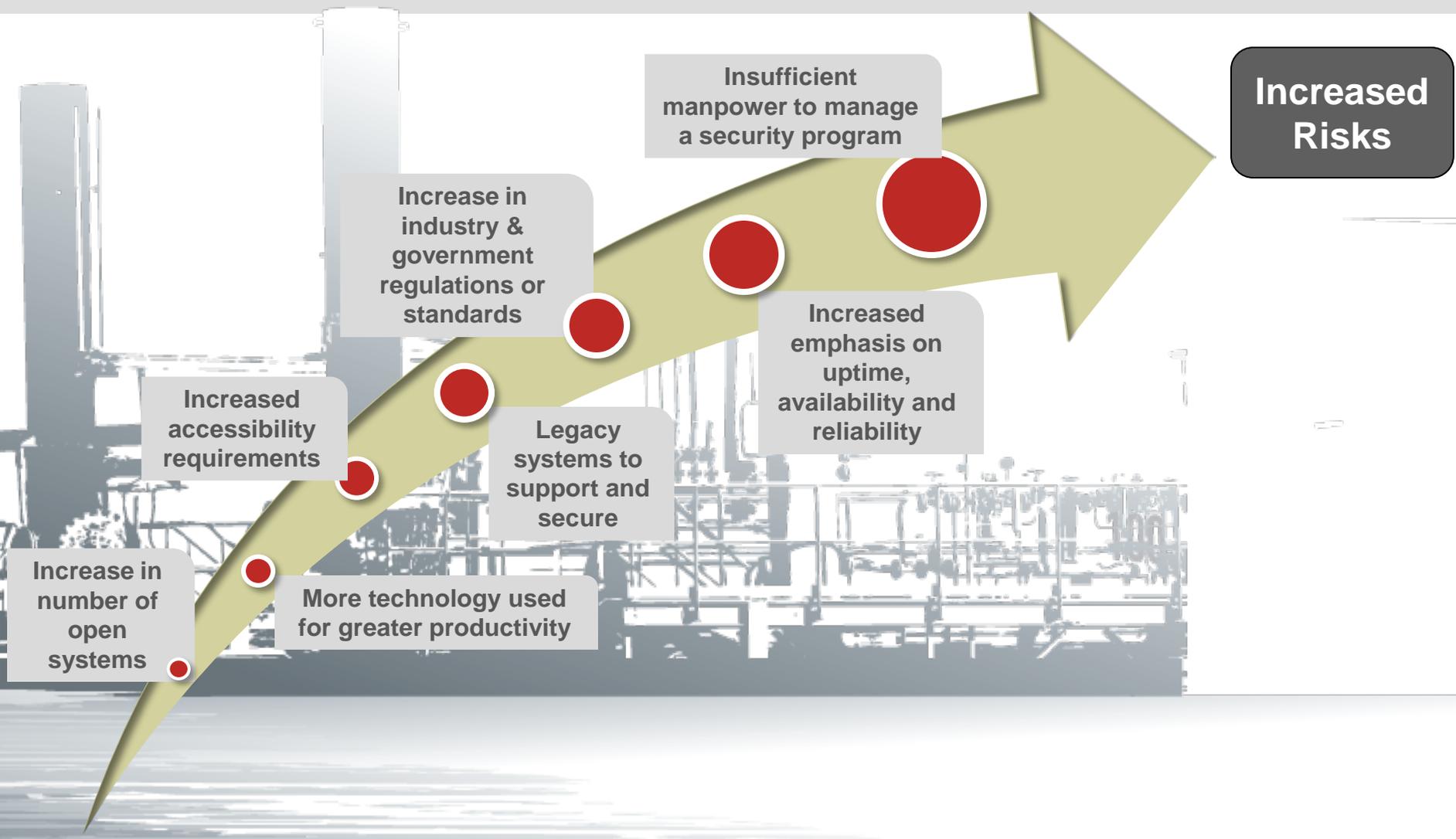
**Projects**

200+ projects combining IT best practices, current regulatory standards and complex process control environments

**Fact**

Honeywell offers hardware independent expert opinions on best practices for cyber security

# INDUSTRIAL CYBER SECURITY CHALLENGES



## Recent Stats

- Recent McAfee report states that:
  - Cost of downtime from major attacks exceeds \$6 million US per day
  - Cyber attacks on critical utilities systems have nearly doubled since 2009
  - 80% of the water, gas and energy firms around the World reported that hackers had compromised their security systems in the past year

**Adoption of security measures continues to grow. However unlike the threats and vulnerabilities, the adoption rate is improving slowly.**

Source: <http://www.mcafee.com/us/resources/reports/rp-critical-infrastructure-protection.pdf>

# Impact of a Cyber Security Breach

- Unauthorized access, theft, or misuse of information
- Loss of integrity or reliability of process data and production information
- Loss of system availability
- Process upsets leading to inferior product quality, lost production capacity, compromised process safety or environmental releases
- Equipment damage
- Personal injury
- Violation of legal and regulatory requirements
- Public health and safety

**Cyber security is about ensuring safe, reliable, and expected system behavior**

# NERC CIP for Power Industry

- 1<sup>st</sup> industry to enforce cyber security regulatory requirements in North America
- Cyber security framework for “critical” cyber assets that support the reliable operation of the Bulk Electric System
- 1<sup>st</sup> regulatory standard to have audit measures and penalties in the industrial environment

**\$72,461,986 US in fines  
for non-compliance since adoption**

## NERC CIP STANDARDS

CIP 002 Critical Cyber Assets

CIP 003 Security Management Controls

CIP 004 Personnel & Training

CIP 005 Electronic Security

CIP 006 Physical Security

CIP 007 Systems Security Management

CIP 008 Incident Reporting & Response Plan

CIP 009 Recovery Plans

# NERC CIP Timeline

## 2006

Standards drafting team (SDT) started work on NERC CIP version 1 in 2006

## 2008

Version 1 approved by FERC

*FERC approved on the basis that the drafting team would implement specific changes in a newer version of NERC CIP*

## 2009

Version 1 effective June for Transmission and December 31<sup>st</sup> for Generation

Version 2 approved by FERC

*In approving Version 2, FERC ordered some small changes to take effect in 90 days*

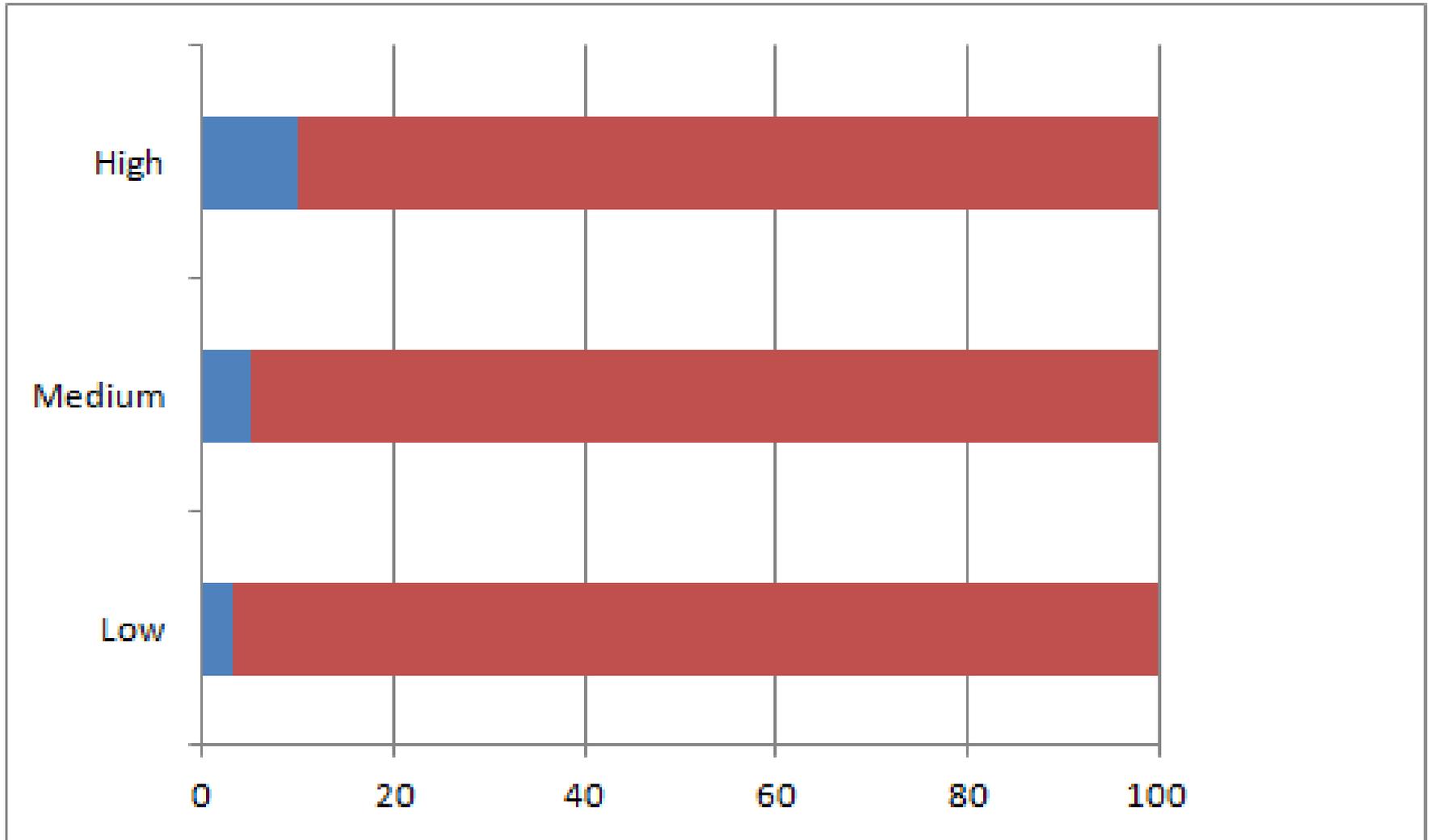
## 2010

Version 2 effective April 1st 2010

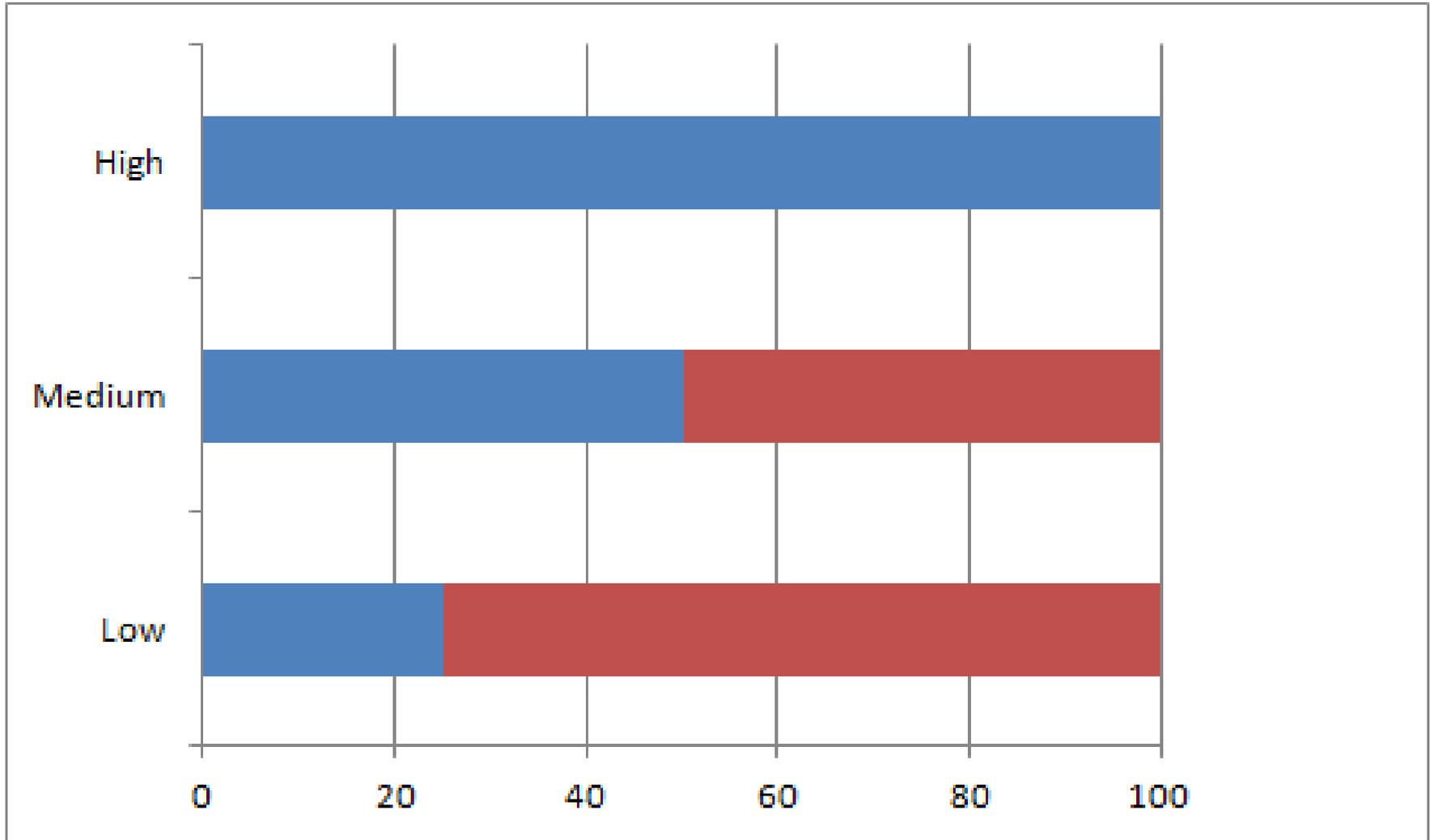
Version 3 approved & effective October  
*(Current version in effect)*

**There is only 17% participation  
with the current version**

# Today's Participation with Version 3



# Future Participation



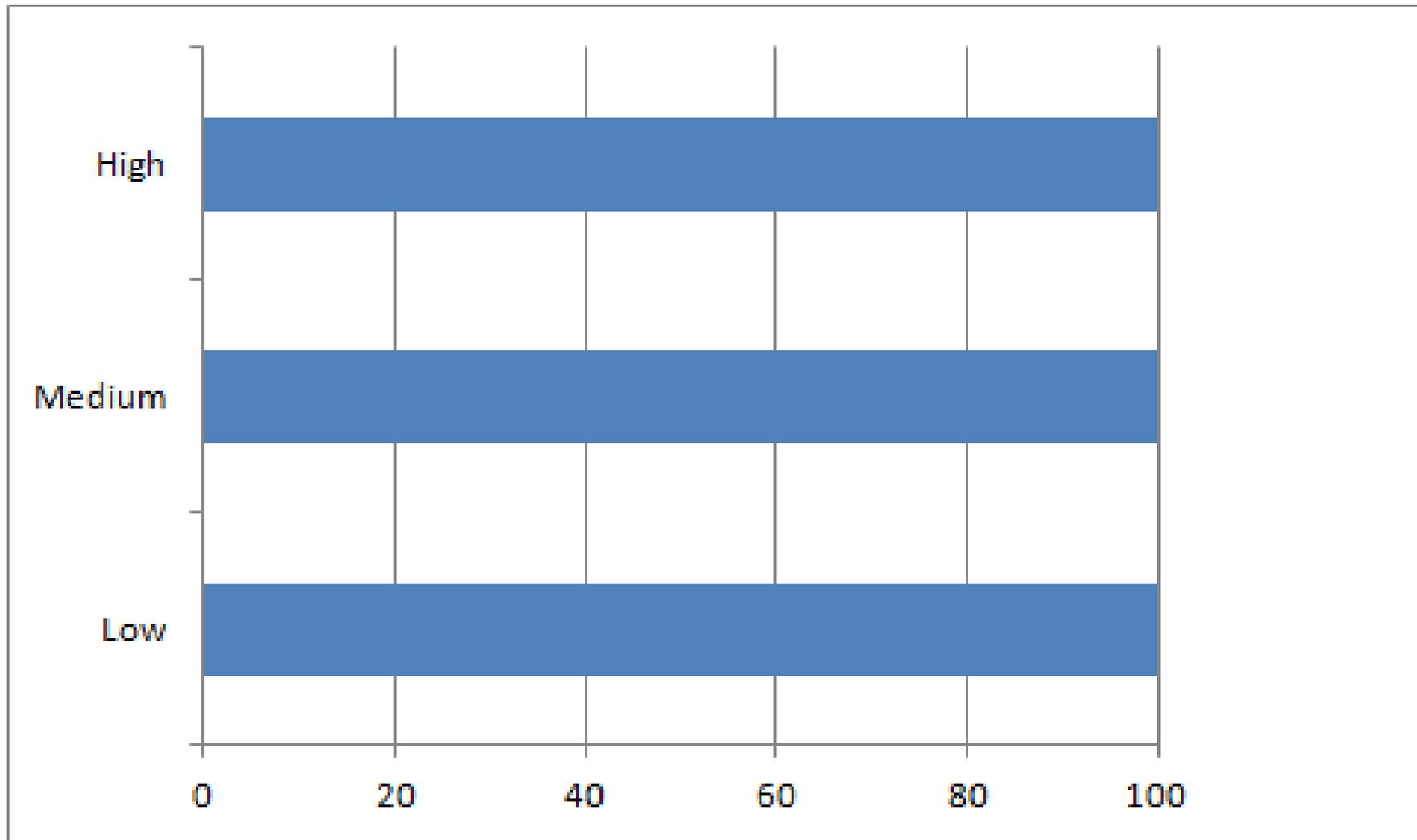
## Version 4

- The problem is the risk-based assessment methodology is subjective
- Need to replace subjective with empirical
  - Version 4 introduces the “bright-line” criteria
  - Designed to expand the number of Bulk Electric System assets designated as critical assets
- FERC has yet to approve version 4

## Version 5

- SDT has started work on version 5 while waiting for FERC to approve Version 4
- Addresses all the specific changes that FERC asked for when approving the first version (version 1)
- Introduced levels of cyber assets:
  - All cyber assets will require a “baseline” level of security controls
  - Higher impact cyber assets will be subject to higher levels of security controls

# End Goal



# Impact on Power Companies

How did power companies approach and accept the standards?

Realistic

Last Minute

Avoidance

Realistic –  
Proactive, jumped on board, took a holistic approach

Last Minute –  
Started to create the building blocks however left majority of the work until last minute and were left scrambling at the 11th hour on December 31, 2009.

Avoidance –  
Used the subjective risk-based assessment methodology to avoid the need to comply

# Mixed Results

- Proactive –
  - Understand the intention the NERC CIP standards
  - Have a effective, holistic security program that successfully reduces security risks
- Last Minute –
  - Racing against the ticking clock significantly increased costs and effort
  - Security program that was thrown together and just “ticks the compliance” checkbox
  - Reduced effectiveness and success of their security program
  - Lack of employee uptake/support
- Avoidance –
  - Have yet to start
  - Will have a lot of work moving forward as the new versions become approved

# The Real Risks

- Organisations' are avoiding the real day-to-day risks of operation that exist regardless of terrorist or other targeted, motivated attack vectors
- Need to consider the risks associated with a far more probable threat vector:
  - inadvertent, non-malicious behavior
- Very high likelihood companies will be hit with unintentional negligent behavior long before they are ever victims of a targeted attack
  - Average user is at work in trusted situations and locations
  - Circumvent security policies without understanding the repercussions and risks

# Today's Reality

- Need to think beyond the bureaucracy of compliance
  - Change the way we think



## Today's Reality

- Embrace the realization that cyber security is about ensuring safe, reliable, and expected system behavior
- Recognize cyber security's crucial role in the reliability and robustness of the networks the critical applications run on
- Cyber security is destined to become entrenched in process control industries in much the same way as the culture of safety

# Long-Term Security Strategy

- Need to move from reactive to proactive
- Use a phased approach to implement a manageable, scalable security program
- Involve multiple work disciplines:  
Operations, Process Control, IT, HR, etc
- Gain support and endorsement from all communities of interest
- Implementing even a baseline security model across your facility increases the likelihood of safe, reliable operations and minimizes potential security incidents

# Long-Term Security Strategy

- Where to start?
  - Start with taking inventory of what is on your plant floor
  - Understand your business risks
  - Understand how the threats are getting in?



Best Practice	NERC CIP	ISO/IEC	Recommended?
Risk-based Assessment for Asset Identification	✓		
Defense-in-depth Strategy	✓	✓	✓
Authentication & Authorization	✓	✓	✓
User Access Management	✓	✓	✓
System Hardening	✓	✓	✓
Anti-virus	✓	✓	✓
Patch Management	✓	✓	✓
Physical Security	✓	✓	✓
Back-up Strategy	✓	✓	✓
Incident Response Plan	✓	✓	✓
Monitoring & Logging	✓	✓	✓
Training & Awareness	✓	✓	✓
Change Management Procedure	✓	✓	✓
Annual Vulnerability Assessments	✓		

# Security is more than just technology!



**Security is *More* than just a Firewall**

# People, Process, and Technology



## Benefits

- Allows time to socialise the concept of security over time
- Phased approach allows time for trial and error and to incorporate lessons learned into the security program
- Spreads the cost and effort over time
- Increases overall effectiveness
- Increases employee support
- Positions your organisation well once a regulatory standard is mandated for your industry

# Questions



Stacey Kelly

[stacey.kelly@honeywell.com](mailto:stacey.kelly@honeywell.com)

Office: +1 780 945 4085

Mobile: +1 780 499 2188

Follow us: [twitter.com/rickkaun](https://twitter.com/rickkaun)

Visit our blog: <http://insecurity.matrikon.com>

Website: <http://www.matrikon.com/security>

