Cyber Solutions
Customer presentation 2019
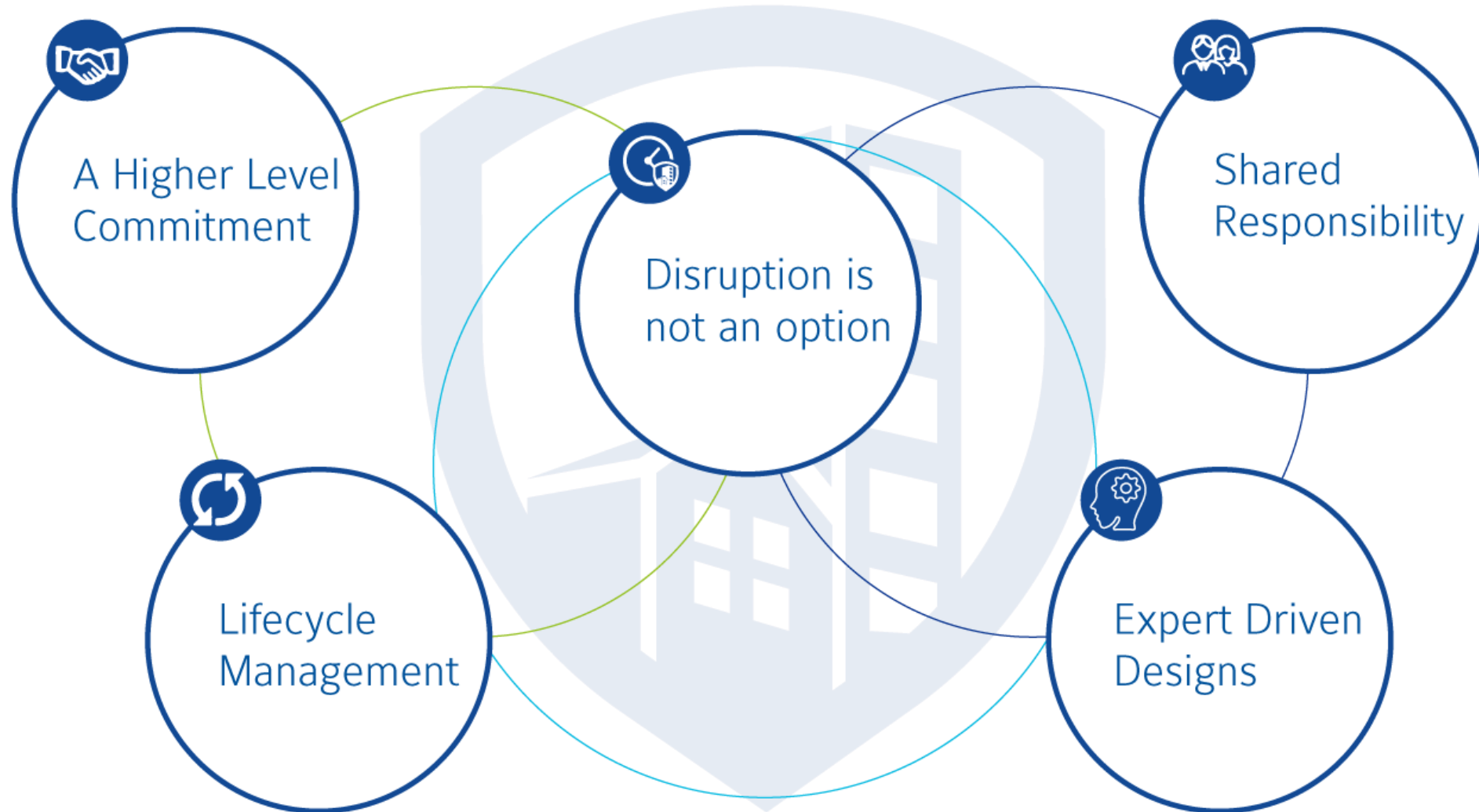
Cyber solutions from a trusted partner

Johnson Controls

Cyber Solutions

A Higher Level Commitment

Lifecycle Management

Disruption is not an option

Shared Responsibility

Expert Driven Designs

Johnson Controls

Cyber Solutions

Cyber Solutions to address concerns where disruption is not an option…

the safety of ….

- **Children…**
- **Travelers…**
- **Employees…**
- **Customers…**

the protection of ….

- **Privacy…**
- **Sensitive information…**
- **Trade secrets…**

the continuity of business ….

- **Workplace efficiency…**
- **Critical operations…**
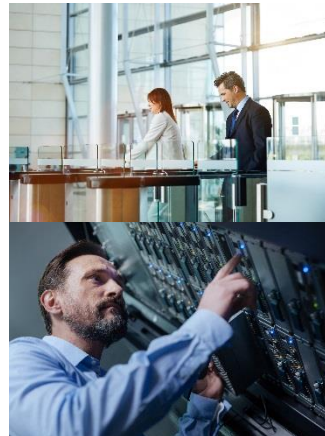
the compliance with policies and regulations….

- **Government…**
- **Healthcare…**
- **Banking and Finance…**
- **Privacy Laws…**

the retention of customers ….

- **Maintaining brand reputation …**
- **Assuring quality…**
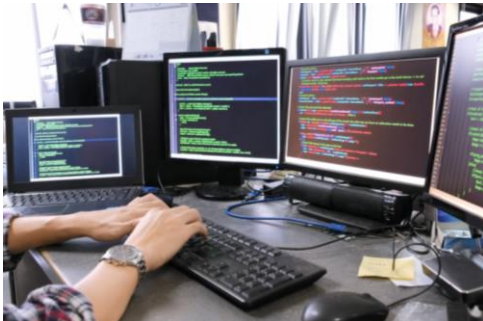- **Meeting service levels…**

Johnson Controls

Cyber Solutions

Holistic Methodology

Governed by Policies and Supported by a Dedicated Global Product Security Team…

Secure development	Deployment services	Rapid Response
• Designed to standards by experts	• Assisted compliance	• PRISRT managed formal response

Disruption is Not an Option

A Higher Level Commitment

Expert Driven Designs

Lifecycle Management

Shared Responsibility

Cyber Solutions – for OT environments

Traditional IT concerns meet unique OT requirements…

Operation Technologies (OT) are the systems and components which keep a building operational. OT systems include:

- Physical Access Control
- Intrusion
- Video
- Building Management
- Fire Protection

OT systems can work with Information Technologies (IT), but often have unique needs.

C

I **A**
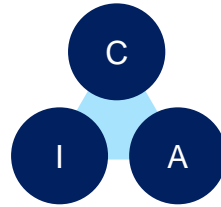
(C) Confidentiality – Sensitive or private data is stolen

(I) Integrity – Data is changed or the connecting device is impersonated.

(A) Availability – Resources are forced offline impacting business continuity

Physical Security System Threats

Violation of **privacy, identity theft**

Unauthorized access to building, **missed events**, **fake video** streams

Designed to protect life cannot fail - must be available 24/7.

! **+ Safety**: cyber-physical attacks on the rise

…cybersecurity measures must be designed to account for the unique role of OT systems

Johnson Controls

Cyber Solution

Attacks continue to disrupt people and businesses…

External Threats		Internal Threats		Unintentional Threats		Cyber Risk
Internet Hackers	**+**	Disgruntled employees	**+**	Poorly managed systems	**=**	

April 2018 - City of Atlanta was a victim of a ransomware cyberattack. Customers were unable to pay bills and parking violations online, departments had to process requests manually and services, such as hiring employees, were suspended.

May 2018 – TeenSafe.com a mobile app which touts itself as a "secure" monitoring app aimed at parents, was responsible for servers which were publicly exposed, leaking parental email addresses, child Apple IDs, device names, and device identifiers.

July 2018 - SingHealth– over 1.5 million healthcare patient records, including Prime Minister Lee Hsien Loong, were stolen.
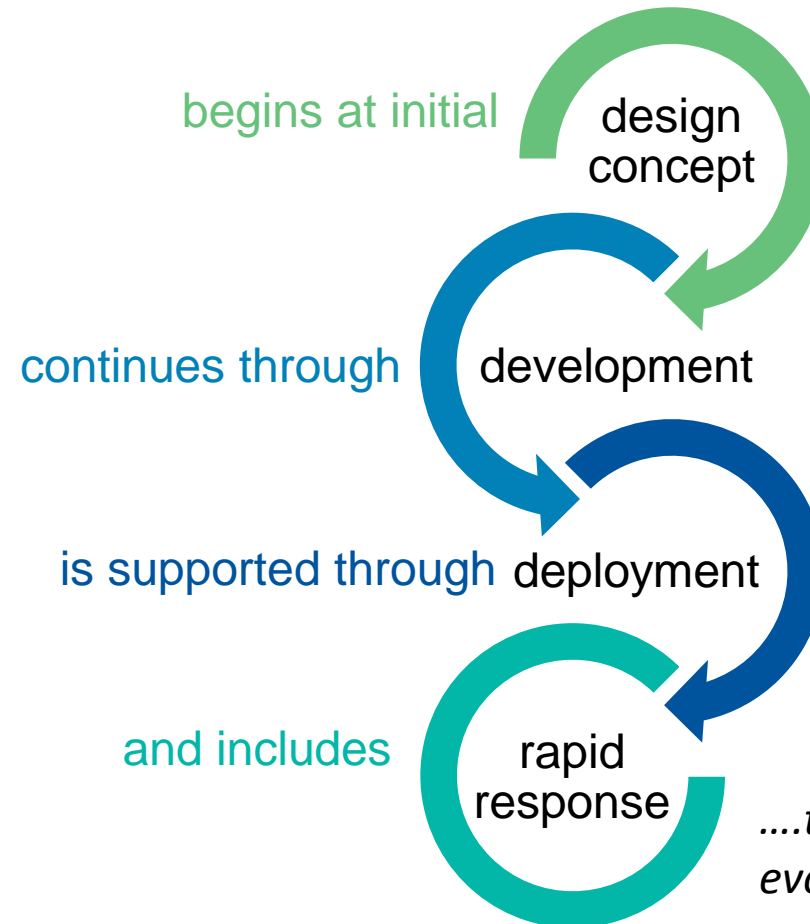
Johnson Controls

Our holistic cyber mindset…

Johnson Controls' approach to cyber protection is aimed at providing peace of mind to our customers.

We provide and support cyber resilient systems with a range of capabilities to complement the diverse security needs of our customers.

- Policy driven
- Strong governance
- Discipline execution
- Continuous enhancement

begins at initial **design concept**

continues through **development**

is supported through **deployment**

and includes **rapid response**

….to meet the comprehensive and evolving cybersecurity environments.

Johnson Controls

Cyber Solutions

We have invested in establishing a centralized dedicated Global Product Security team that is focused on managing our cyber practices with governance to enforce compliance.

Having engineering teams trained in cybersecurity has given Johnson Controls an advantage in developing products that consider cybersecurity within its core design.

Our certified cybersecurity experts work to validate designs using the latest recognized industry standards and practices.

Our cybersecurity experts have certifications including, but limited to ….

CISSP — Certified Information Systems Security Professional

CSSLP — Certified Secure Software Lifecycle Professional

CCSP — Certified Cloud Security Professional

CEH™ — Certified Ethical Hacker

*Expert driven cybersecurity designs provide the forethought required to **reduce risk**..*

Johnson Controls

Cyber Solutions

Our cyber protection approach begins with the **design**, **development** and **testing**.

Based on Microsoft Software Development Lifecycle (SDL)

Design

Develop

Require

Test

Respond

Johnson Controls

Cyber Solutions
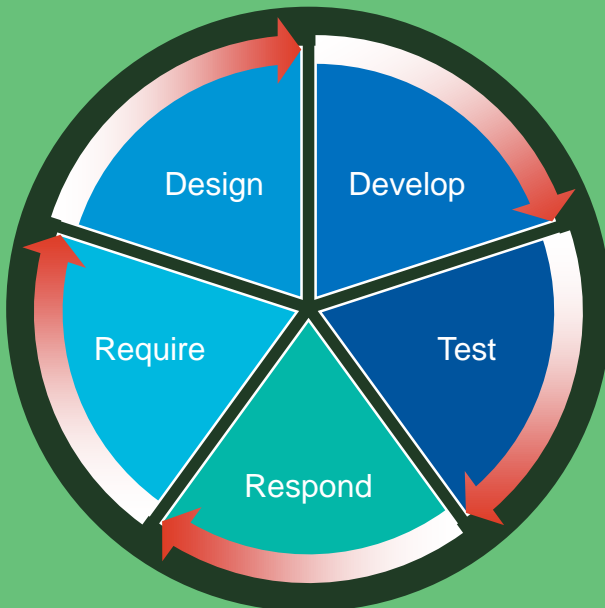
Our cyber protection approach begins with the **design**, **development** and **testing**.

Based on Microsoft Software Development Lifecycle (SDL)
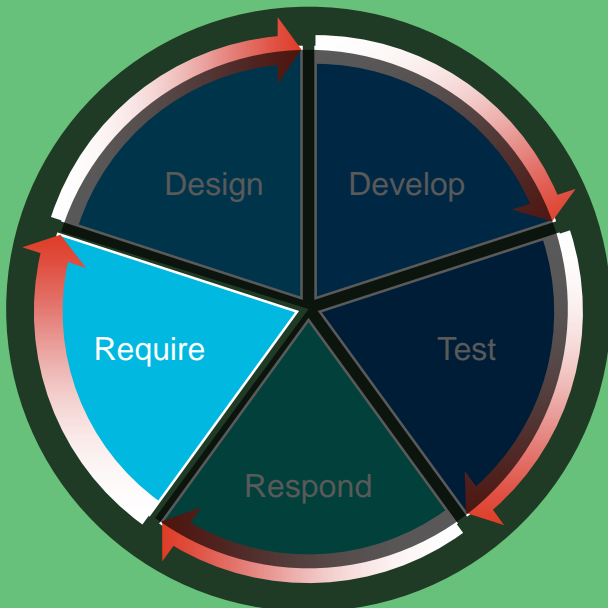

Security Requirements

- Baseline requirements address 14 core threat categories including:
  - Authentication, access control, session management, data protection and malicious input handling.

- Requirements derived from established cybersecurity standards and tailored for our domain including:
  - OWASP — Open Web Application Security Project
  - NIST SP 800-53r5 Security and privacy Controls for Information Systems and Organizations

  - ISA/IEC 62443 — **Section 3-3** Requirements for Systems Security Assurance (SSA) Certification
    Section 4-1 Requirements for Security Development Lifecycle Assurance (SDLA) Certification
    Section 4-2 Requirements for Embedded Device Security Assurance (EDSA) Certification

  - UFC 4-010-06 — Department of Defense Unified Facilities Criteria

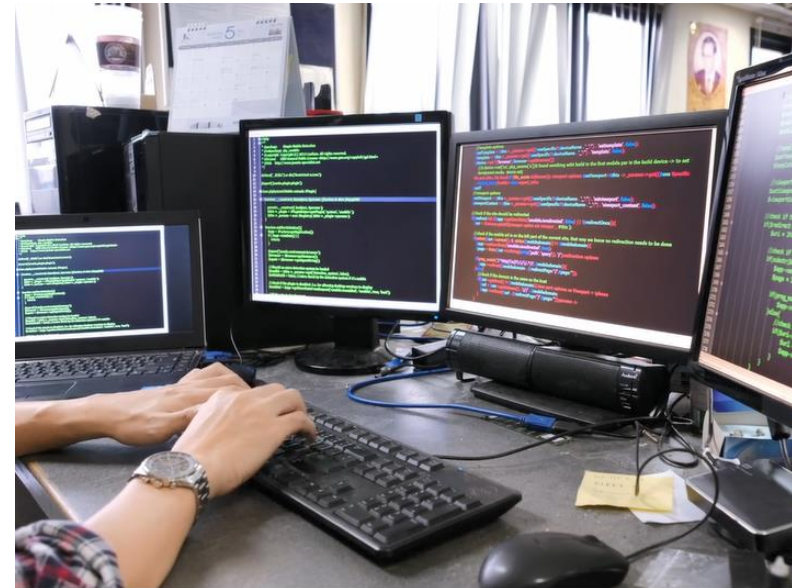- Security requirements addressed in the initial project phase.

Cyber Solutions

Our cyber protection approach begins with the **design**, **development** and **testing**.

Based on Microsoft Software Development Lifecycle (SDL)
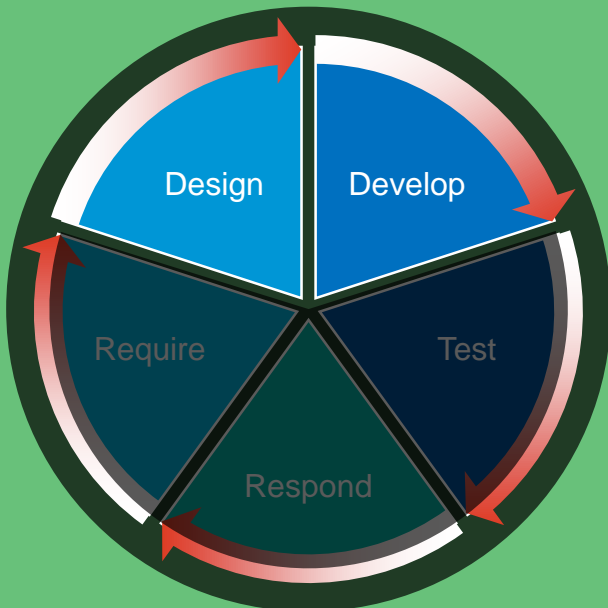
**Security Design & Development**
- Security champions and architects assigned to each project
- Designs are assessed using threat modeling
- Suppliers undergo validation
- Code reviews are conducted throughout development

Cyber Solutions

Our cyber protection approach begins with the **design**, **development** and **testing**.

Based on Microsoft Software Development Lifecycle (SDL)
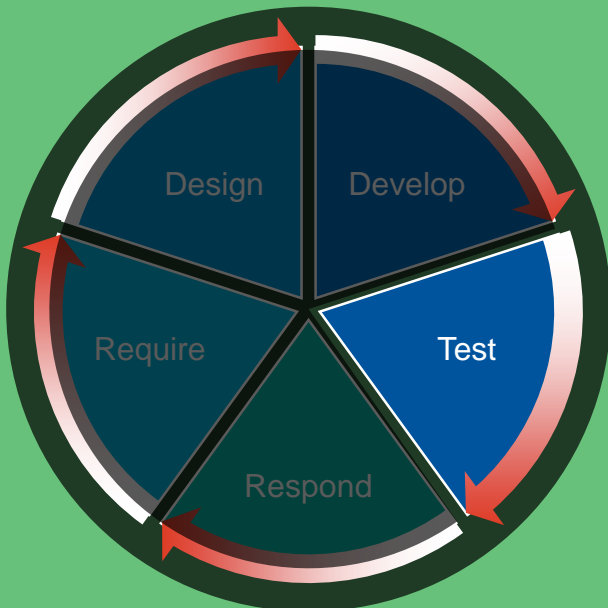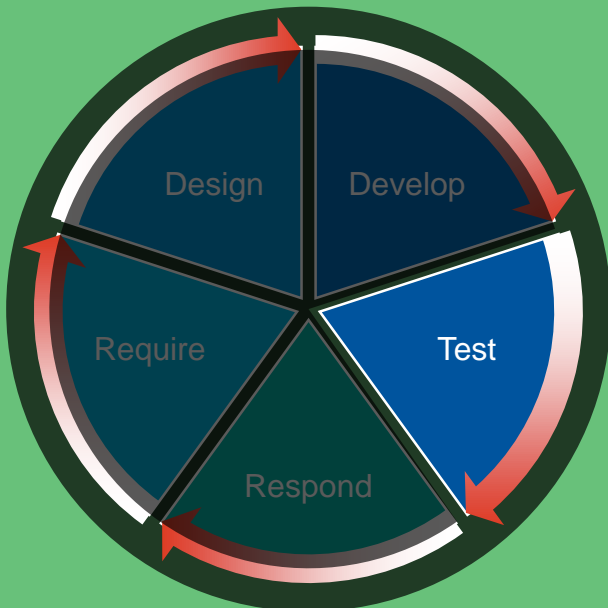

Testing

- In-house continuous testing is leveraged to identify issues early.

- Testing is geared to each product's function and target environments may include:
  - Source code assessments
  - Vulnerability scans
  - Fuzz testing
  - Penetration testing

- Multiple tools and strategies are utilized to reduce risk including:
  - Unit test frameworks
  - Continuous Integration / Continuous Deployment (CI/CD)
  - Static analysis tools
  - Open source software scanning

- Third party penetration is conducted as required.

Cyber Solutions

Our cyber protection approach begins with the **design**, **development** and **testing**.

Based on Microsoft Software Development Lifecycle (SDL)

Testing

- Cybersecurity certifications and approvals provide specific security assurance as required
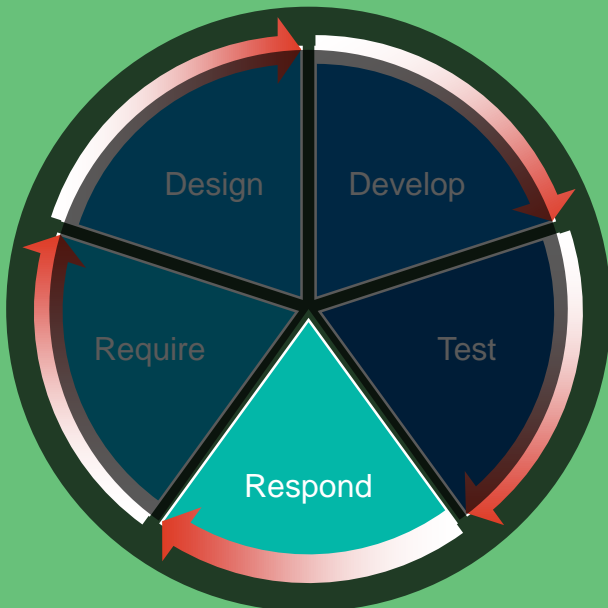
Cyber Solutions

Our cyber protection approach begins with the **design**, **development** and **testing**.

Based on Microsoft Software Development Lifecycle (SDL)

Rapid Response

- Through the rapid incident response service, our dedicated cybersecurity team quickly assesses new threats and vulnerabilities and advises customers on how they may reduce their cybersecurity exposure

    - Product security incident response (PSIR)
    - Advisories
    - Patches / updates as required
    - Threat and trend monitoring

- The plan and supporting material conform to
    - ISO 30111:2013(E) "vulnerability handling process"
    - ISO 29147:2014(E) "vulnerability discloser"

- Responsible disclosure
    - MITRE CVE numbering authority

- Advisories are available on the Cyber Protection website: https://tycosecurityproducts.com/CyberProtection

ISO International Organization for Standardization

ICS-CERT
INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

CVE
Common Vulnerabilities & Exposures

Johnson Controls

Cyber Solutions

Since protecting against cyber threats is a shared responsibility, we engage in market facing programs to provide customer engagement, education, and thought leadership to help our customers achieve success in their mission of a more secure system.

- Market facing programs
- Promote customer engagement through Customer education
- Compliance guidelines
- Cybersecurity documentation
- Thought leadership
  (active on cybersecurity community boards, speaking events, articles, etc.

- **ISA Secure** – Johnson Controls is a strategic voting member of ISA Secure Compliance Institute
  - Conformity assessments to ISA/IEC 62443

- **FIRST** – Full member of the Forum of Incident Response and Security Teams (FIRST)

- **OWASP** – Contributing member of OWASP

- **MITRE** – CVE Numbering authority

- Content is available on the Cyber Protection website:
  https://tycosecurityproducts.com/CyberProtection

Cyber Solutions

The benefits of a comprehensive program

Policy Driven Team	Cybersecurity is not an afterthought
Secure Development	Product designed to be more cyber-resilient
Testing	Testing focused on discovering and addressing critical vulnerability before release
Education	Empowers customer to approach cyber risks pragmatically
Incident response	Dedicated cybersecurity team quickly assesses new threats and vulnerabilities and advises customer on how to reduce their cybersecurity risk

Disruption is Not an Option

A Higher Level Commitment

Expert Driven Designs

Lifecycle Management

Shared Responsibility

Johnson Controls

The product security program is applied to all brands