Which is Job #1: Quality or Cybersecurity?

American Society for Quality
2/22/2024

Agenda

01 Speaker and Session Introduction

02 Ethics, Assurances, and Fraud

03 Risk Management Framework

04 Introduction to Cyber Security

05 Questions and Answers

06 Closing Remarks

Speaker Introduction

Cybersecurity Advisor

Donald.Borsay@Cyberbuyer.io

Donald@qpsinc.com

TECH CITY ADVISORS

CHANGE THE FUTURE

Work

1. 40+ years in Information Technology
2. 20+ years in Information Security
3. Industries: technology services, insurance, gaming, defense, education, government services, and manufacturing.

COYOTE BROWN

Education/Certification

1. MS in Information Assurance @ Norwich University
2. BS in Computer Science @ University of Rhode Island
3. ISACA Certified Information Systems Auditor (CISA)
4. CompTIA Security+

QPS

MAKING BOTTOM LINE IMPACT

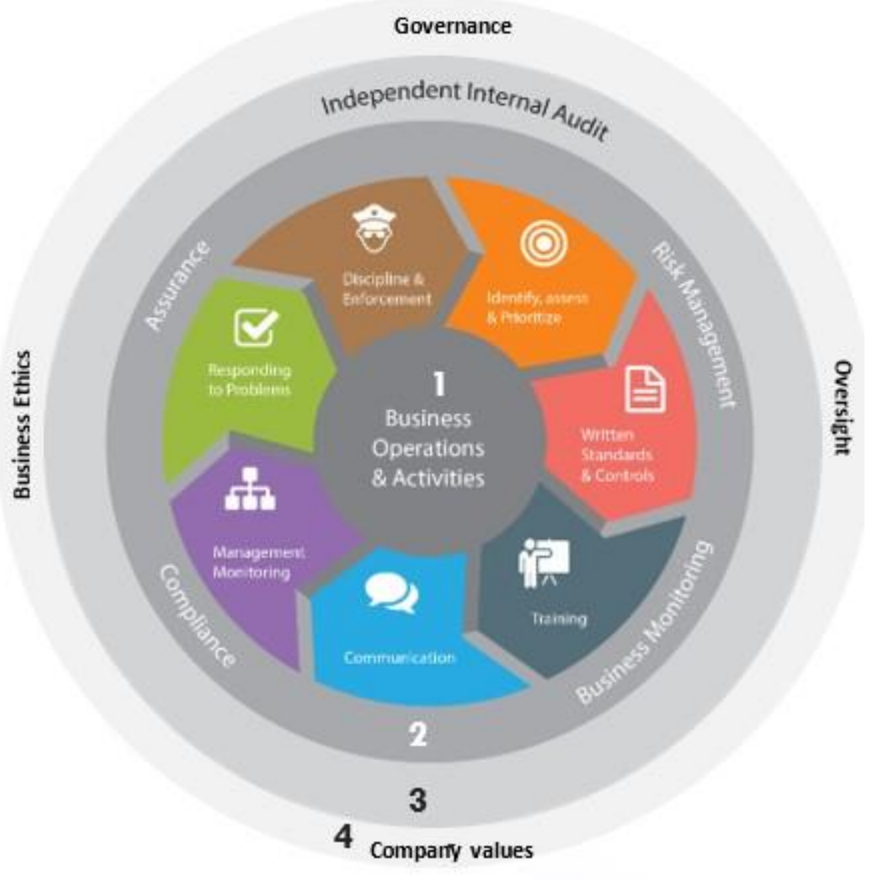
Session Introduction

Ethics, Assuances, and Fraud

Professional Conduct & Controls

Can only ASSURE what you can CONTROL!

1. Assess and Identify Risks
2. Establish standards and procedures.
3. Train to develop skillls and awaness.
4. Communicate importance.
5. Monitor threats and perfoormance.
6. Handle incidents and problems.
7. Disipline and enforce.



Credit: Stealth Africa

Provide assurance of the integrity and origin of quality results so that the integrity and origin can be verified and validated by a third party.

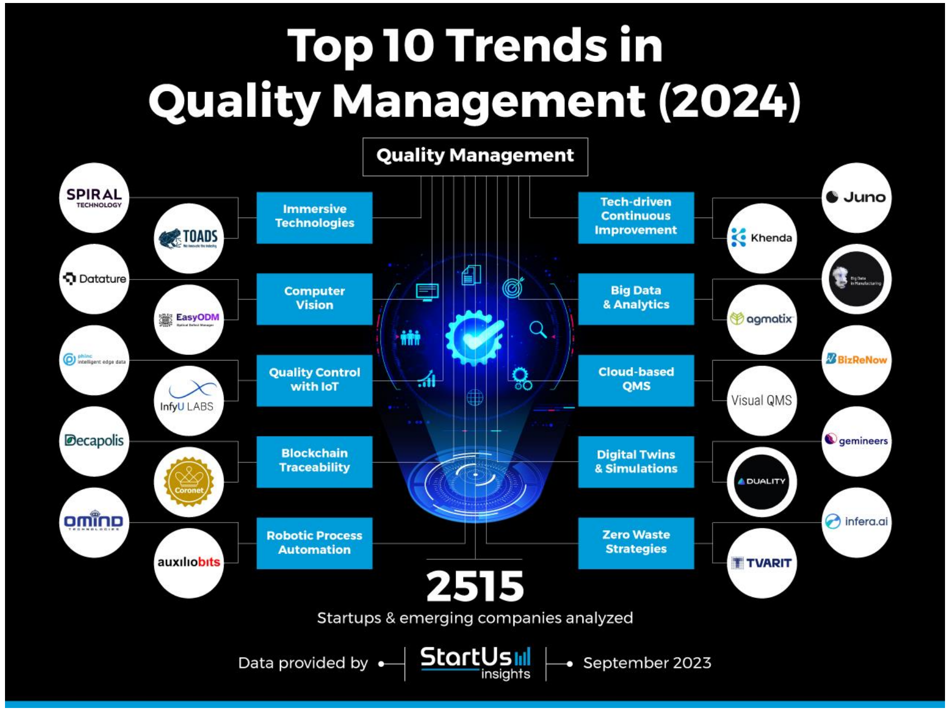
Assurance can be through ATTESTATION, DEMONSTRATION, or TEST.

Cyber – New Business Risk

Quality & IT = Cyber Risk

Quality Management

1. Immersive Technologies
2. Tech-driven Continuous Improvement
3. Computer Vision
4. Big Data & Analytics
5. Quality Control w/IoT
6. Cloud-based QMS
7. Blockchain Traceability
8. Digital Twins & Simulations
9. Robotic Process Automation
10. Zero Waste Strategies



Credit: Startus Insights

Business Risk = Strategic + Regulatory + Financial + <u>OPERATIONAL</u>

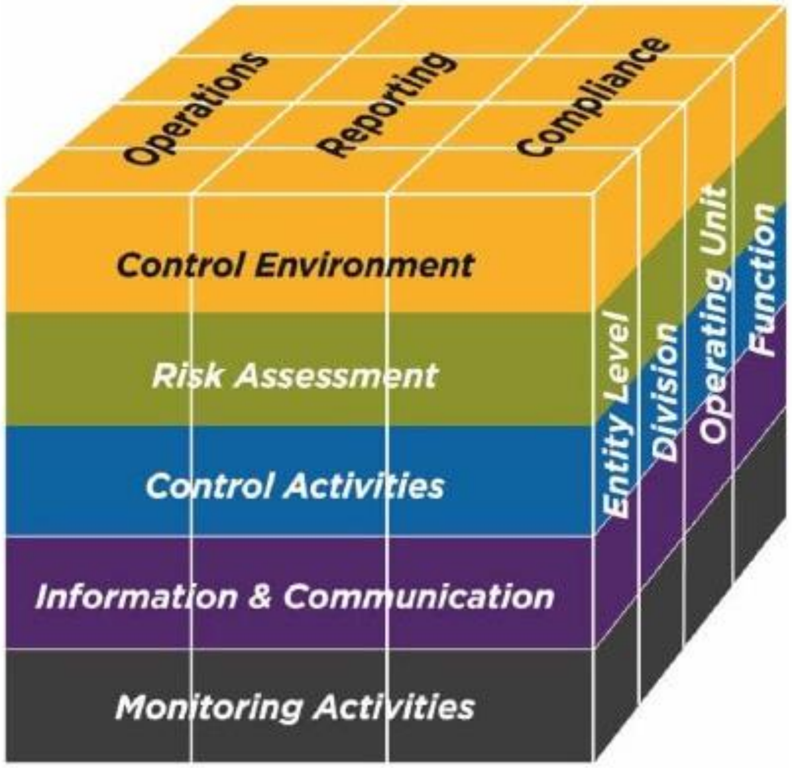
Cyber – New Business Risk

Rise in Cyber-Physical Attacks

- Advances in computer and networking technologies, as well as dependency on interconnected cyber-physical components.
- Limited research on the vulnerability of QC components.
- Legacy tools can be exploited, new tools not being built with cybersecurity in mind.

Managing Cyber Risk

- Same risk management process.
- Cybersecurity SME
  - Different control activities.
  - Different controls.
  - Information about Technology.
    - Cyber Threats
  - Monitoring of usage and threats.



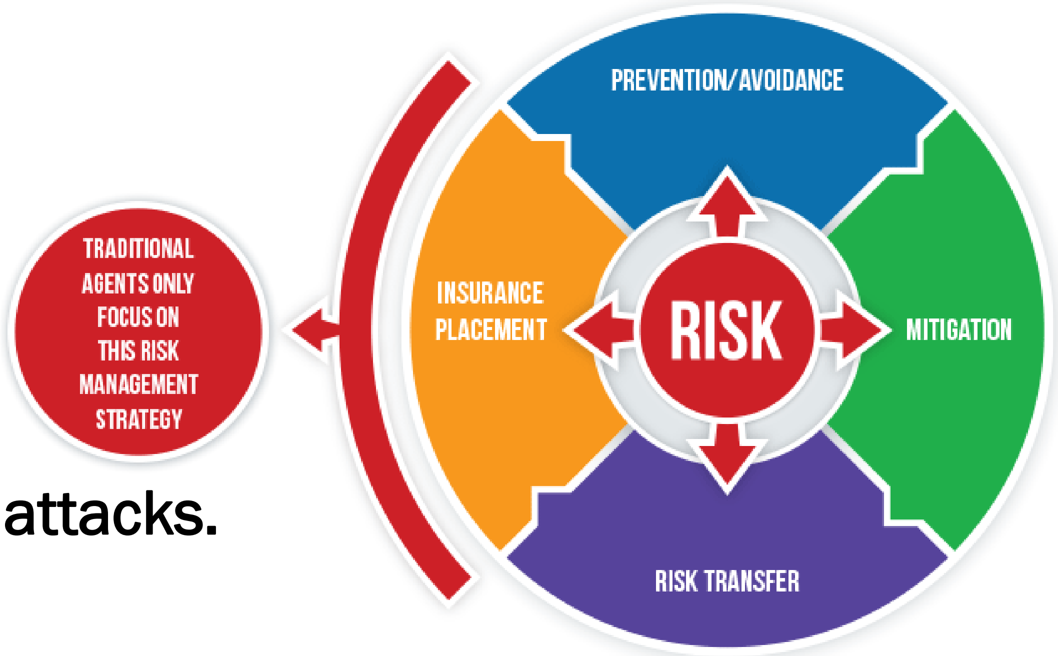
Credit: KnowledgeLeader

Designated Owner: Chief Information Security Officer (CISO)

Detailed Program: Planned Controls, Status, and Risks

Risks Too Big to Self-Insure

- 12% upsurge in cyber claims
- 72% spike in claims severity
- 60% of claims due to Ransomware attacks.



Credit: IronRisk Strategies

- **Increases in insurance demand in short term to outpace supply.**
  - Requires longer-term thinking mixed with near-term action.
  - Insurance is important, but only part of the broader cyber security discussion.

Need a Designated Owner

Threats:

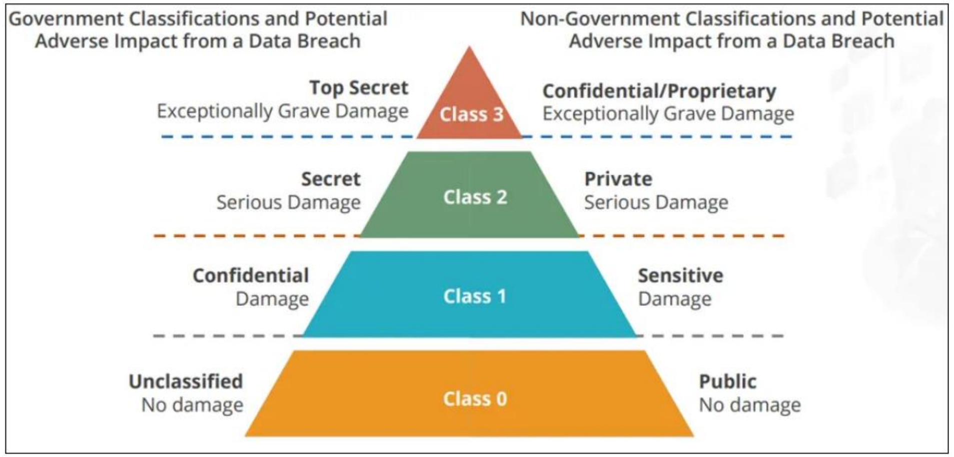
- Difficulty managing requirements.
- Rapid change in threats, operations
- No governance / oversight.
- Lack of expertise in writing policy.
- Suppliers may be weakest link.

Credit: Bitsight

Best Practices:

- Establish a fractional CISO / CPO
  - Policy Management
  - Threat Management
  - Compliance
  - Supplier Management

Protect Sensitive Assets First


Government Classifications and Potential Adverse Impact from a Data Breach
Non-Government Classifications and Potential Adverse Impact from a Data Breach
Top Secret
Exceptionally Grave Damage
Class 3
Confidential/Proprietary
Exceptionally Grave Damage
Secret
Serious Damage
Class 2
Private
Serious Damage
Confidential
Damage
Class 1
Sensitive
Damage
Unclassified
No damage
Class 0
Public
No damage

Credit: IronRisk Strategies

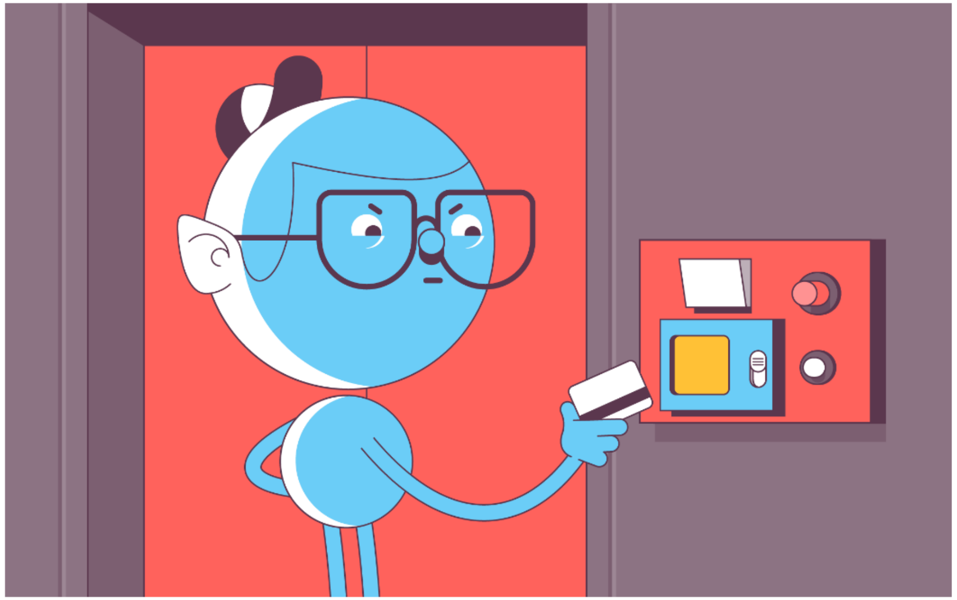
Threats:

- Staff does not know what is important.
- No handling instructions.
- Regulated assets lack proper protection.
- Assets lost or stolen.

Best Practices:

- Classification scheme – public, internal, confidential, restricted.
- Establish an asset inventory.
- Establish a default classification and label everything else.
- Establish handling guidelines per classification.
- Establish retention rules and disposal procedures.

Value is in Access, so is the Risk



Credit: SSLS.COM

Threats:

- Too much access by default.
- Crimes not traceable to individuals.
- Compromised passwords reused.
- Huge impact from single compromised account.

Best Practices:

- Business user access form to document access changes.
- Establish templates for access rights per user role.
- Tie generic accounts to the software that uses them.
- Regularly review access at intervals based upon role risk.
- Monitor access and escalate suspicous behavior.

Be Responsive and Thorough

Credit: Healthcare IT News

Threats:

- Sharp increase in breaches.
- Breaches also more severe.
- Penalties for underreported breaches.
- Response delay compounds impact.

Best Practices:

- Train users on how to detect and report an incident.
- Prepare for likely incidents before they happen.
- Establish breach notification procedures.
- Gather lessons learned to minimize impact on future occurances.

Be Resilent to Likely Impacts

Threats:

- Cut or Insufficient Power
- Poor environment for IT devices.
- IT device failure.
- Network/communication failure.
- Cloud or service provider failure.

Credit: OpsCentre

Best Practices:

- Perform business impact analysis.
- Identify critical resources to business operations.
- Design for resiliency when possible.
- Establish recovery contingencies for likely disasters.

Build Culture Supportive of Cybersecurity

Credit: InformationSecurityProgram.com

Threats:

- Hire staff with criminal history.
- Assets lost/stolen when staff leave company.
- New hires unfamiliar with policy or cybersecurity basics.
- Staff given responsibilities without appropriate training.
- No policy enforcement or procedures for disiplinary action.

Best Practices:

- Check backgrounds before hire.
- Etablish clear conditions for employement.
- Train staff.to provide situational awareness and develop skills.
- Seek return of assets when empliyees leave.

Protect On-Premise Assets

Credit: GeeksForGeeks.org

Threats:

- Damage to equipment.
- Social engineering of staff.
- Unauthorized access to sensitive assets.
- Theft of equipment

Best Practices:

- Establish perimeter security to your facilities.
- Establish secure areas per asset classification.
- Issue/wear badges for internal staff and guests.
- Challenge individuals in secure areas without badges.
- Monitor access points 24x7.
- Clear desk, lock draws and cabinets.

Harden Your Systems

Credit: Healthcare IT News

Threats:

- Non-compliance
- Unnecessary Services
- Vulnerable Services
- Cascading Impact Due to Design

Best Practices:

- Verify systems meet security requirements before purchase/use.
- Ensure all systems are in asset inventory.
- Use stripped down, turn-key systems in public areas.
- Limit access to the most sensitive servers to select workstations.
- Place core network equipment and cables is restricted areas.

Limit Access Through Your Network

Credit: Cisco

Threats:

- Attackers and Threats on Internet
- Attacks may use required connections.
- Network could enable access to vulnerable assets.
- Access riules not static, requires monitoring/adjustment.

Best Practices:

- Install modern network gear with behavioral threat analysis.
- Establish network zones per cleassification.
- Filter access to the most sensitive zones.
- Use fractional network security engineer to maintain.

Introdction to Cybersecurity Operations

Maintain Security in Operations

Top Cybersecurity Threats in 2023
PRIVACY CONCERNS WITH SEMI-AUTONOMOUS VEHICLES
EVOLVING RANSOMWARE STRATEGIES
CRYPTOJACKING
MOBILE ATTACKS
SOPHISTICATED PHISHING
STATE SPONSORED ATTACKS
CLOUD VULNERABILITY
VULNERABLE SMART MEDICAL DEVICES
CYBER-PHYSICAL ATTACKS
SHORTAGE OF CYBER SECURITY PROFESSIONALS
DATA BREACHES
THIRD PARTY VULNERABILITIES
SOCIAL ENGINEERING
LOT ATTACKS
REMOTE WORK ENVIRONMENTS

Threats:

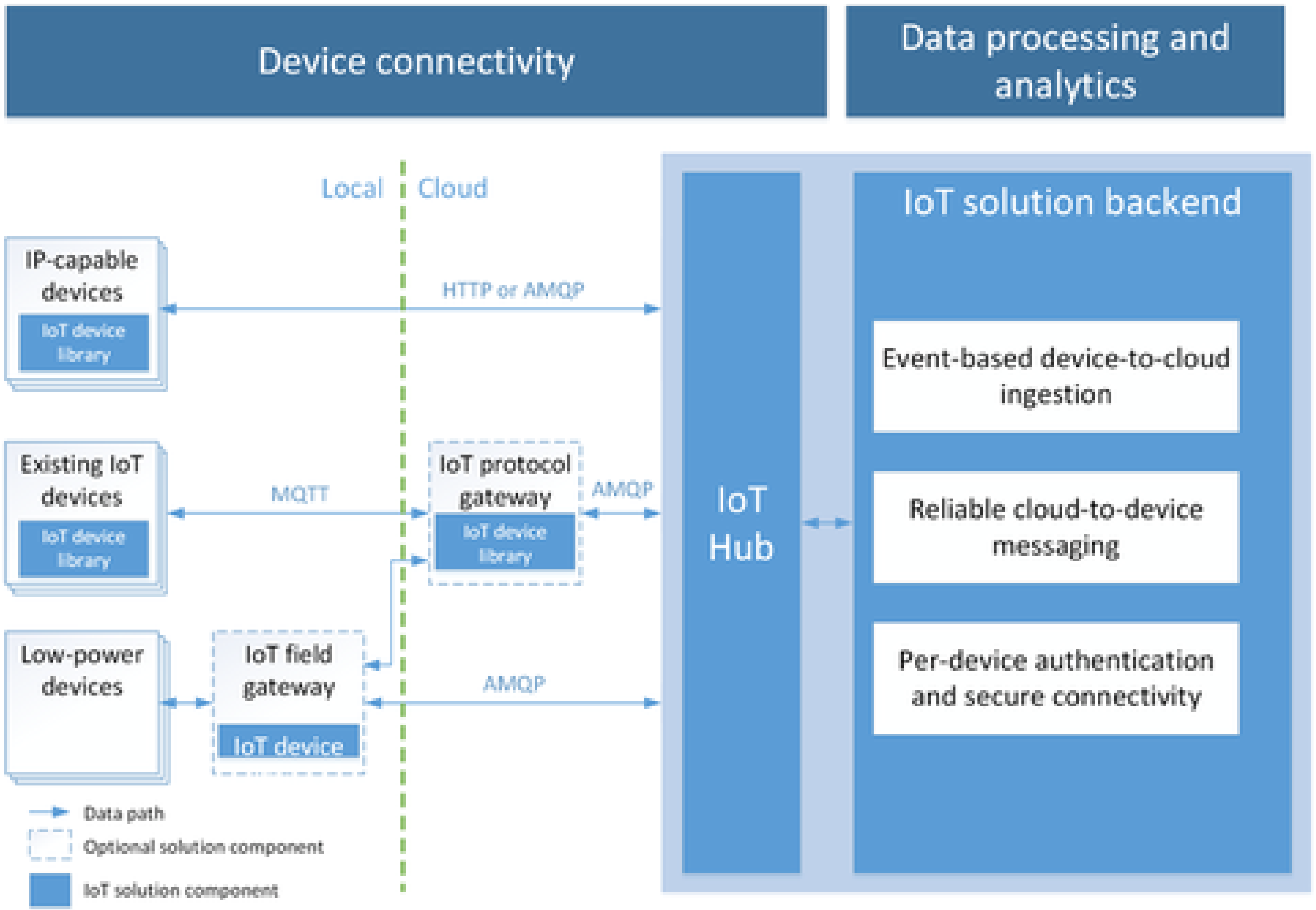
- Rise in Ransomware
- Compromised/inadequate backups.
- Rise in Zero-Day vulnerabilities..
- Lack of control of software.

Best Practices:

- Inventory and control software, including dependent vendors.
- Clarify operational roles vs. that of service provider.
- Verify backup plan to BCP, test backups.
- Manage technical vulnerability based upon severity.
- Monitor capacities to avoid exhaustion and business impact.

Quality Control in Manufacturing
Exploring the Cyber Risk

Quality Control Architecture



Device connectivity

Data processing and analytics

Local | Cloud

IP-capable devices
IoT device library

HTTP or AMQP

Existing IoT devices
IoT device library

MQTT

IoT protocol gateway
IoT device library

AMQP

Low-power devices

IoT field gateway
IoT device

AMQP

IoT Hub

IoT solution backend

Event-based device-to-cloud ingestion

Reliable cloud-to-device messaging

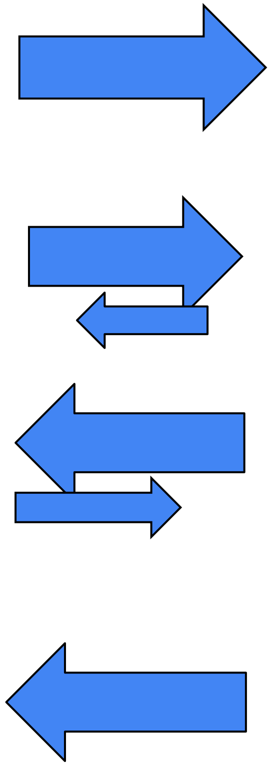
Per-device authentication and secure connectivity

Data path

Optional solution component

IoT solution component

Integration Patterns



Telemetry – device pushes data to backend;

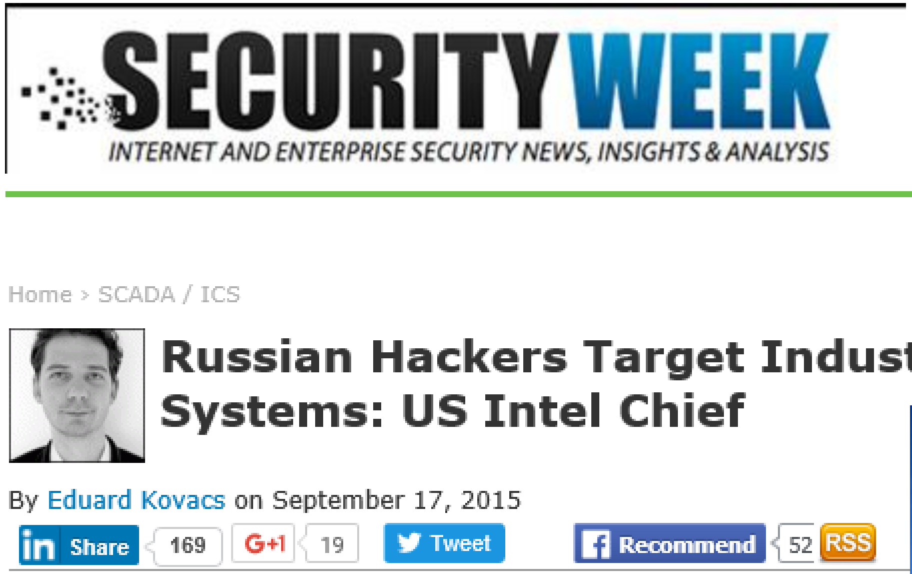
Inquiries – device periodically checks in;

Command and Control – backend instructs device to perform specific activities;

Notifications – backend provides updates to device.

Critical Infrastructures – National Security

- Chemical Sector
- Commercial Facilities Sector
- Communications Sector
- Critical Manufacturing Sector
- Defense Industrial Base Sector
- Dams Sector
- Emergency Services Sector
- Energy Sector
- Financial Services Sector
- Food and Agriculture Sector
- Government Facilities Sector
- Healthcare and Public Health Sector
- Information Technology Sector
- Nuclear Reactors, Materials, and Waste Sector
- Transportation Systems Sector
- Water and Wastewater Systems Sector



SECURITYWEEK
INTERNET AND ENTERPRISE SECURITY NEWS, INSIGHTS & ANALYSIS

Home › SCADA / ICS

Russian Hackers Target Industrial Control Systems: US Intel Chief

By Eduard Kovacs on September 17, 2015