INTERTEK HVAC CYBER SECURITY WEBINAR

May 2019

Joe Dawson, Principal Software Security Analyst

EWA-Canada

intertek ewa canada

01 Introduction

02 The Threat Landscape

03 Threat Mitigation Measures / HVAC Cyber examples

04 Our Place in the Connected World

05 Device Security Standards / Approaches

06 How we Help Clients

01

INTRODUCTION

A brief history of EWA-Canada and Intertek's role as a global leader in cyber security

INTERTEK AND CYBER SECURITY

EWA-Canada Incorporated in 1988

- Established to provide electronic warfare (EW) engineering support to the Canadian military

Expanded full-time into IT security in mid 90's

- First Canadian member of the Forum of International Security and Response Teams (FIRST) in 1997
- Established the CanCERT in 1998
- Infrastructure and vulnerability assessments and penetration testing since 1996

Testing cyber security in products for 19+ years

- Accredited as a Common Criteria (CC) lab in 1999
- Accredited as a cryptographic and security test (FIPS 140-2) lab in 2001
- Conducting compliance and certification testing for payment terminals since 2003

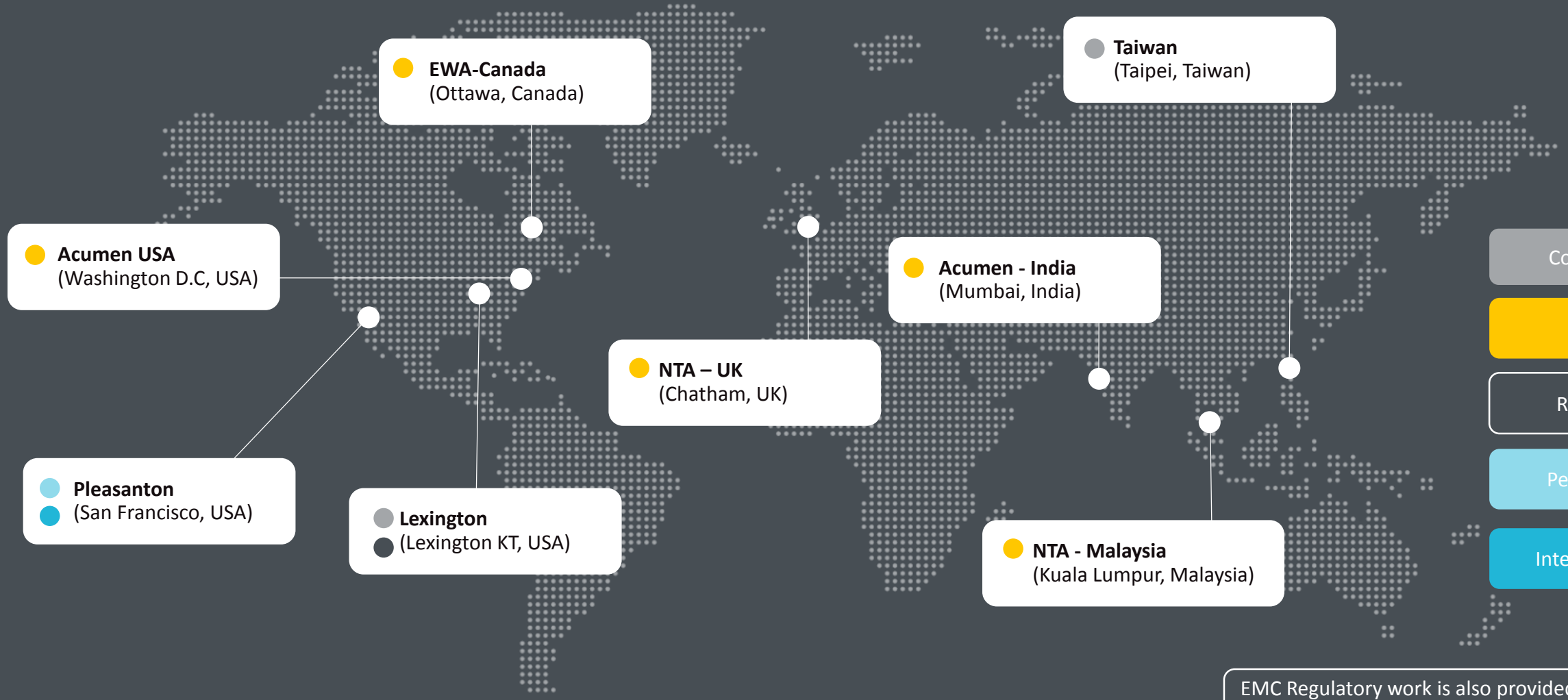
Joining the Intertek Team

- Acquires EWA-Canada - 2016
- Intertek Acquires Acumen Security - 2017
- Intertek Acquires NTA Monitor - 2018

GBL STRATEGY: A SINGLE PROVIDER WITH COMPLETE SPREAD OF SOLUTIONS ALLOWING NEW & EXISTING CLIENTS TO LAUNCH CONNECTED HVAC PRODUCTS

5 Core Connected World Competencies	Intertek's customer promise
1. Security	Ensuring security of data and operations
2. Connectivity	Ensuring Network Access
3. Regulatory	Facilitating Market Access
4. Performance	Testing your Performance Promise
5. Interoperability	Validating the Interfaces between Connected Devices

OUR GLOBAL CONNECTED WORLD NETWORK AND CAPABILITIES
>260 EMPLOYEES IN 8 LOCATIONS



- Connectivity
- Security
- Regulatory
- Performance
- Interoperability

EMC Regulatory work is also provided globally by the Electrical GBL

CORE COMPETENCIES

Current Business Lines	Example Work Scopes
Risk Management and Emerging Technologies	• IoT product testing • including binary and source code static analysis • Threat Risk Assessments (TRAs) of systems, services and/or applications • Best practices security configuration reviews • Vulnerability assessments / penetration testing • Risk assessments
Operations Assurance	• Threat information sharing via the Canadian Cyber Threat Exchange (CCTX) • Design/Operate Certificate Authorities (CAs) • Operate ASV Validation Lab for PCI
Payment Assurance	• Payment Certification Testing of devices • Including binary code static analysis

Product Evaluation **(includes CC, FIPS)**	• ISO/IEC 15408 Common Criteria product security evaluations under the following national schemes:
	  • Canada
	  • Sweden
	  • Spain
	• Cryptographic Module & Algorithm security testing:
	  • FIPS 140-2, ISO 19790 (includes source code analysis)

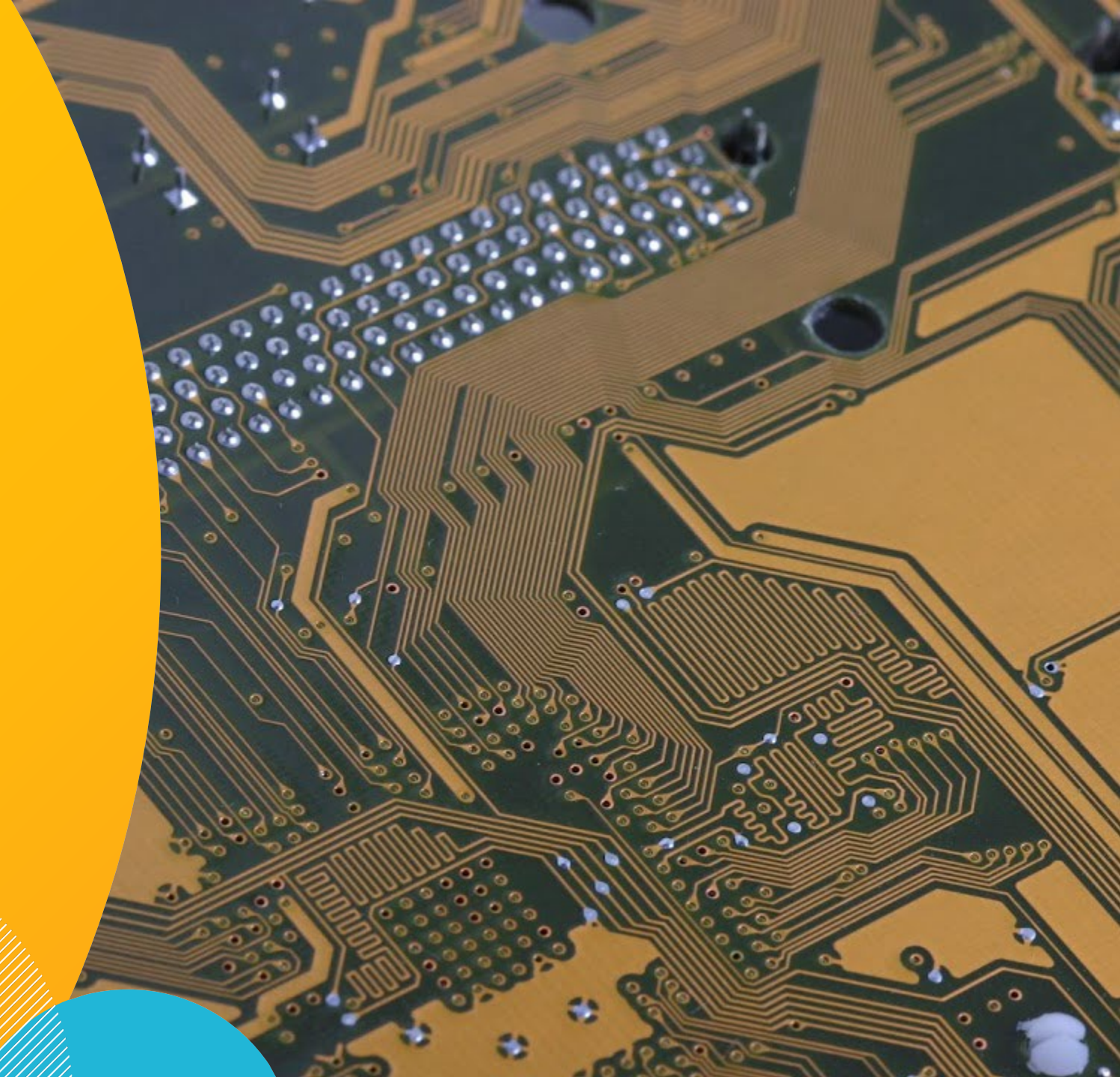
High Assurance	• Detailed security assessment and testing of telecom device software and firmware • Identify security weaknesses • Binary and source code static analysis

intertek ewa canada

02

THE THREAT LANDSCAPE

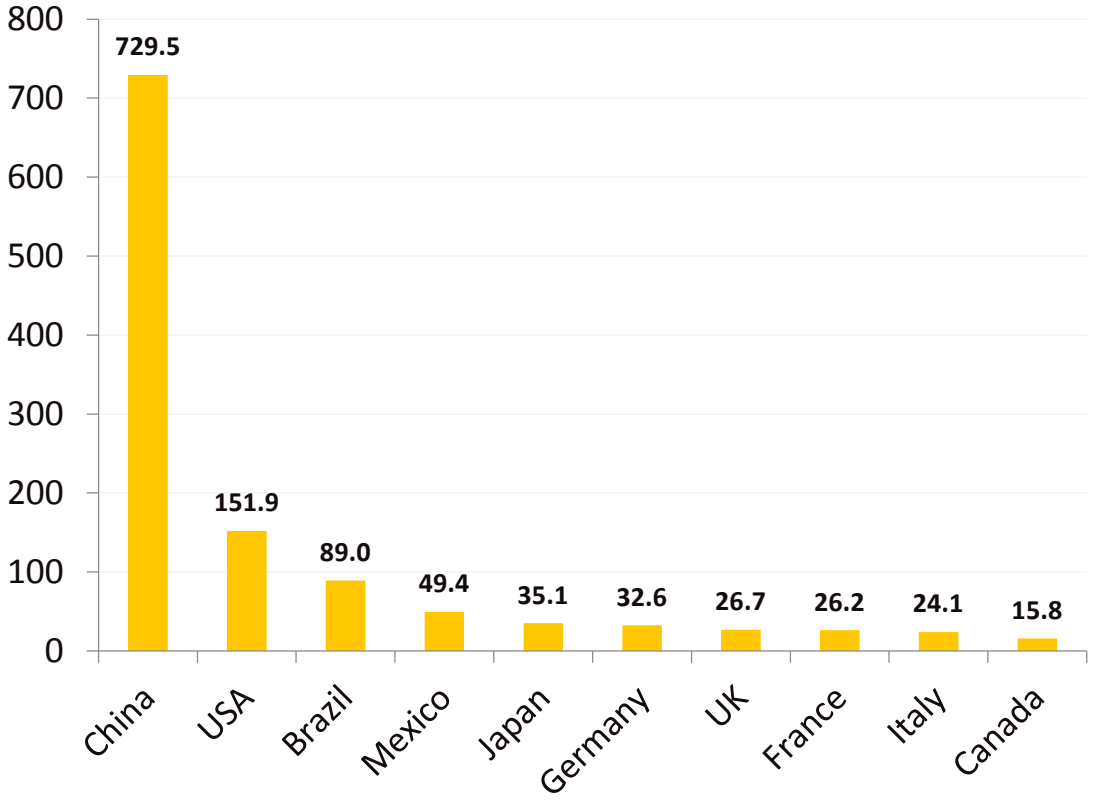
A survey of significant threats to organizations



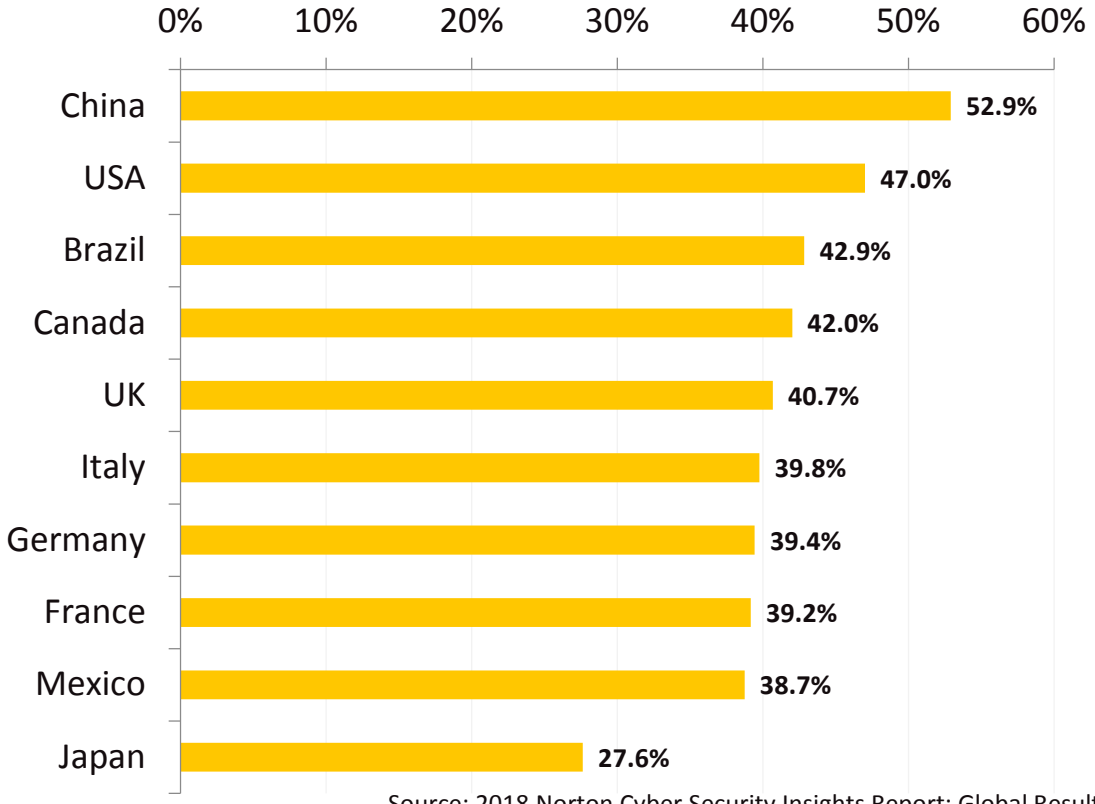
THREAT LANDSCAPE
GLOBAL CYBER CRIME

More than 867 million adults in 16 countries were the victims of cyber crime in 2018

"Top 10" Countries (Millions of People)



"Top 10 Countries (% of Total Population)



Source: 2018 Norton Cyber Security Insights Report: Global Results

THREAT LANDSCAPE
INTERNET OF THINGS

Malware

Botnets

Ransomware

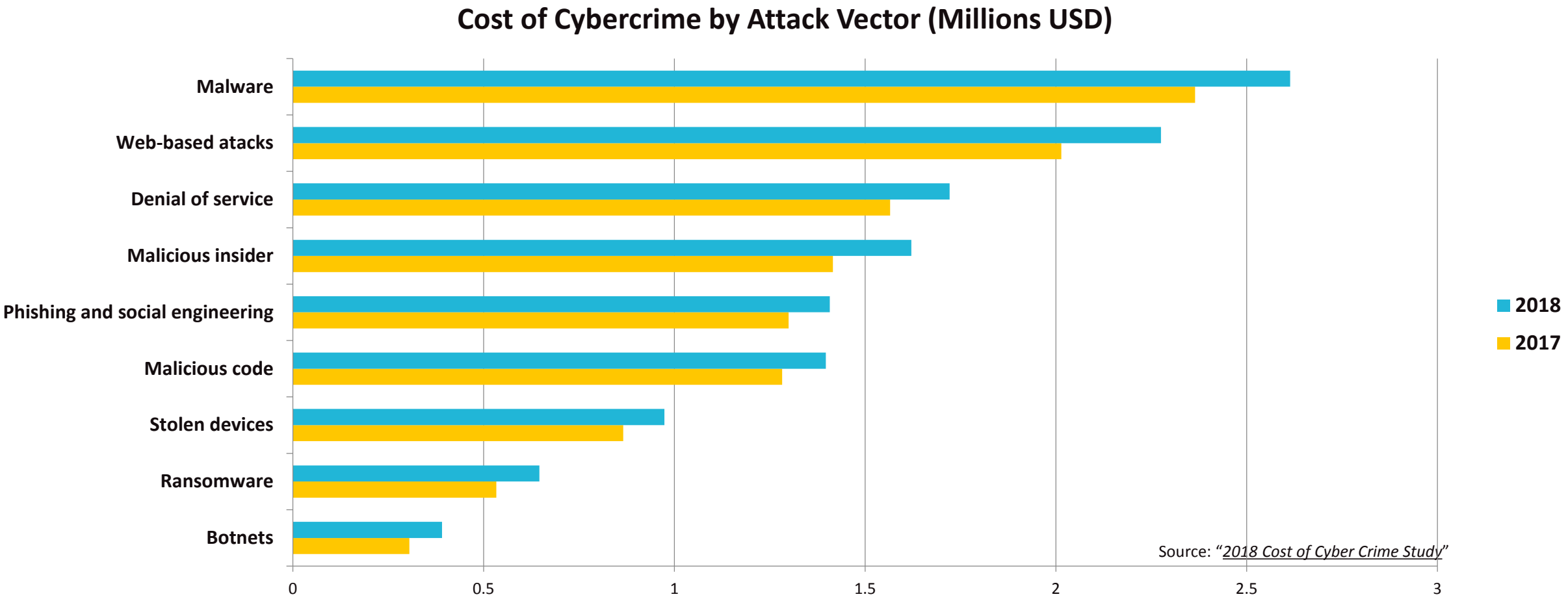
Cryptojacking

DoS

Phishing

THREAT LANDSCAPE

MOST COMMON ATTACK VECTORS EXPERIENCED BY ORGANIZATIONS



EXAMPLE: EVOLUTION OF IOT MALWARE THREATS

August ’16

Mirai scanned for services using default credentials

September ’17

Malware targets known vulnerabilities in products

(Mirai -> IoT_reaper)

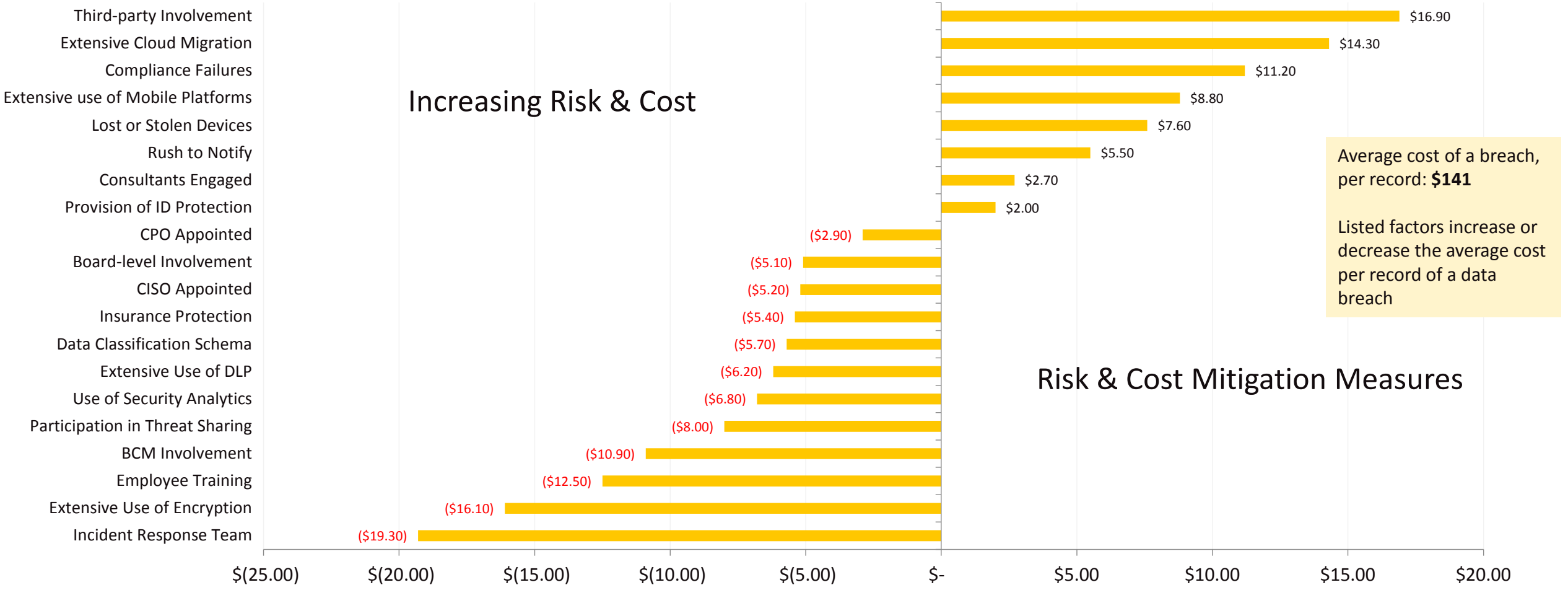
November ‘17

Malware targets zero-day vulnerabilities

(Mirai -> Satori)

Source: https://researchcenter.paloaltonetworks.com/2018/01/unit42-iot-malware-evolves-harvest-bots-exploiting-zero-day-home-router-vulnerability/

DATA BREACH INCIDENT RESPONSE COSTS



Average cost of a breach, per record: **$141**

Listed factors increase or decrease the average cost per record of a data breach

Source: Ponemon Institute's "*2017 Cost of Data Breach Study*"

HVAC CYBER EXAMPLES

HVAC CASE STUDY

- Your company sells a smart Thermostat / HVAC
  - It allows clients to view and modify Temperature / HVAC settings remotely
  - It may also allow your support folks to remotely modify and support the clients Thermostat / HVAC system.
  - Systems like this are often installed on the clients existing networks.
- How do you ensure your clients that your systems are not creating a risk to their networks?
- Who is responsible if your system causes your client systems to be compromised?

HVAC CYBER EXAMPLES

- Qualys has conducted a survey and identified over 55,000 Internet-connected heating systems, lack adequate security
  - In this report Qualys also stated that many high profile systems such as ones supplied to recent Olympics was also vulnerable.

HVAC CYBER EXAMPLES

- In February 2019 a vendor that supplied refrigeration and HVAC projects for Trader Joe's, Whole Foods and BJ's Wholesale Club locations in Pennsylvania, Maryland, Ohio, Virginia and West Virginia was compromised.
  - This vulnerability placed the clients networks at risks.

HVAC CYBER EXAMPLES

- Target Breach 2013 (40 million credit cards)
  - It was announced that hackers had gained access through a HVAC vender to its point-of-sale (POS) payment card readers.
- Home Depot Breach 2014 (70 million credit cards)
  - Company that serviced HVAC systems in Target's headquarters was reported as the source of the breach.

HVAC CYBER EXAMPLES

- Las Vegas Fish Tank
  - A fish tank in the lobby of a hotel had a remotely monitored, thermostat that allowed the company who sold the tank to automatically adjust temperature and salinity, and automate feedings.
  - It also allowed hackers to swipe 10 gigabytes of data from the casino internal network.

- So what can we learn from this?

intertek ewa canada

03

THREAT MITIGATION MEASURES

Steps you can take today to mitigate threat

PROTECTING THE ORGANIZATION: SECURING THE ECOSYSTEM

Start with Secure Products

Products that have undergone rigorous security evaluation against industry accepted standards such as FIPS 140-2, Common Criteria and/or ANSI/UL 2900 / IEC 62443 or equivalent. IEC 62443

Build a secure networking and computing infrastructure using evaluated products

Follow best practices such as NIST Risk Management Framework (RMF), ISO 27001 or other industry specific standards (e.g. PCI-DSS for credit card processing networks).

Ongoing security assessments

A secure ecosystem should be monitored and maintained. Regularly scheduled audits, hiring outside teams for red-teaming (penetration testing, etc.).

Regular security awareness training

Employees should be regularly trained on security best practices as they perform their jobs.

SECURING PRODUCTS: DESIGNING FOR SECURITY / BENEFITS

Adding security after the fact almost never works as intended and always costs more

"Cyber Security Is A Business Risk, Not Just An IT Problem"

- Forbes, 11 October 2017

Vendor	Consumer
• Brand Reputation • Safety and Security • Lower Liability Risk • Sales • Regulatory Approval	• Safety and Security • Privacy • Peace of Mind

Source: Striking a balance between usability and cyber-security in IoT devices, https://web.mit.edu/smadnick/www/wp/2017-12.pdf

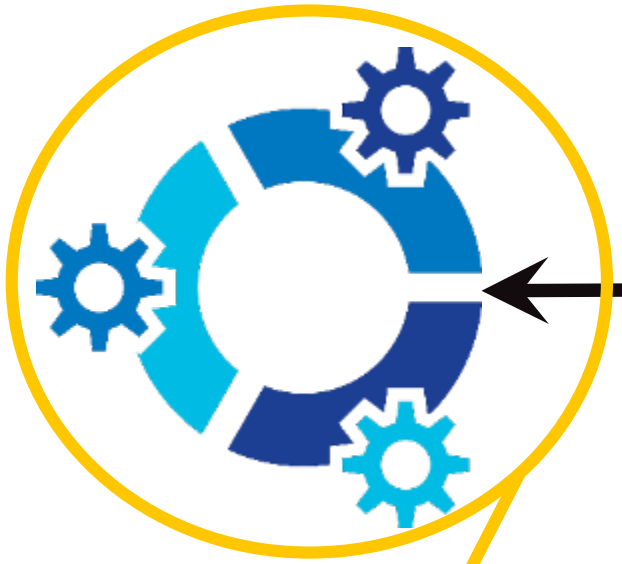
intertek ewa canada

04

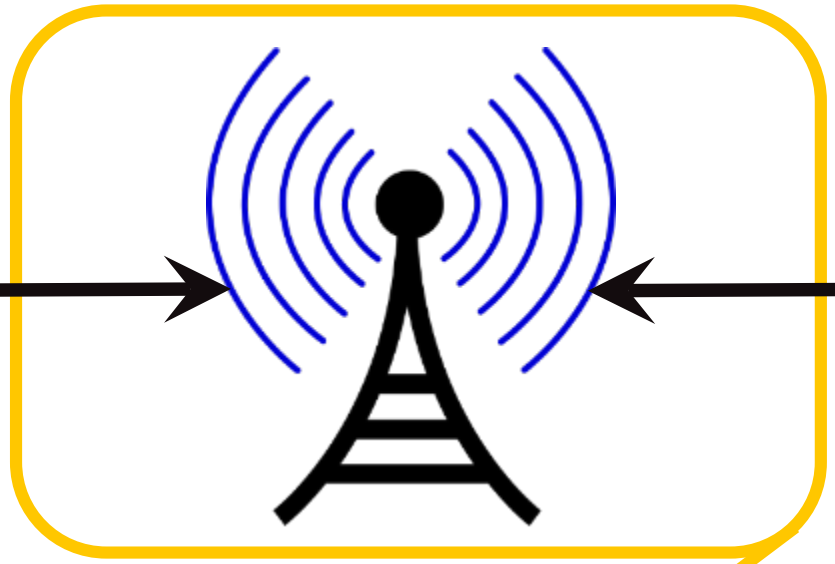
OUR PLACE IN THE CONNECTED WORLD

Leveraging Intertek's experience and expertise

SIMPLE IOT MODEL: SECURITY SCOPE DEFICIENCY IN CURRENT ASSESSMENT MODELS



IoT Services Infrastructure



Communications Infrastructure

Smart Endpoints & User Experience

- Security assessment of the cloud back-end as part of end-to-end assessment is a critical missing component in many of today's IoT security standards

Underlying assumption is that this piece is secure

- Typical scope of an IoT endpoint security test / evaluation
- May not consider the back-end servers and services that the device is connected to
  - often contain user sensitive data

SOLUTION: FULL SCOPE OF TEST AND EVALUATION FOR ENHANCED ASSURANCE

The end-user requires assurance that the:

- smart endpoint has been:
  - tested and certified against all regulatory compliance requirements (safety, EMI/EMC, etc.);
  - confirmed to be interoperable with other devices and platforms (e.g., provides exemplary user experience, etc.); and
  - security tested against industry best-practice standards and requirements;
- communications channel to the back-end service enforces the confidentiality and integrity of all data transferred across it (between the end-device and IoT services infrastructure); and
- IoT services infrastructure has been security tested for assurance that end-user sensitive data is adequately protected against unauthorized disclosure, theft of service, etc.

CONNECTED HVAC PRODUCTS SECURITY CHALLENGES

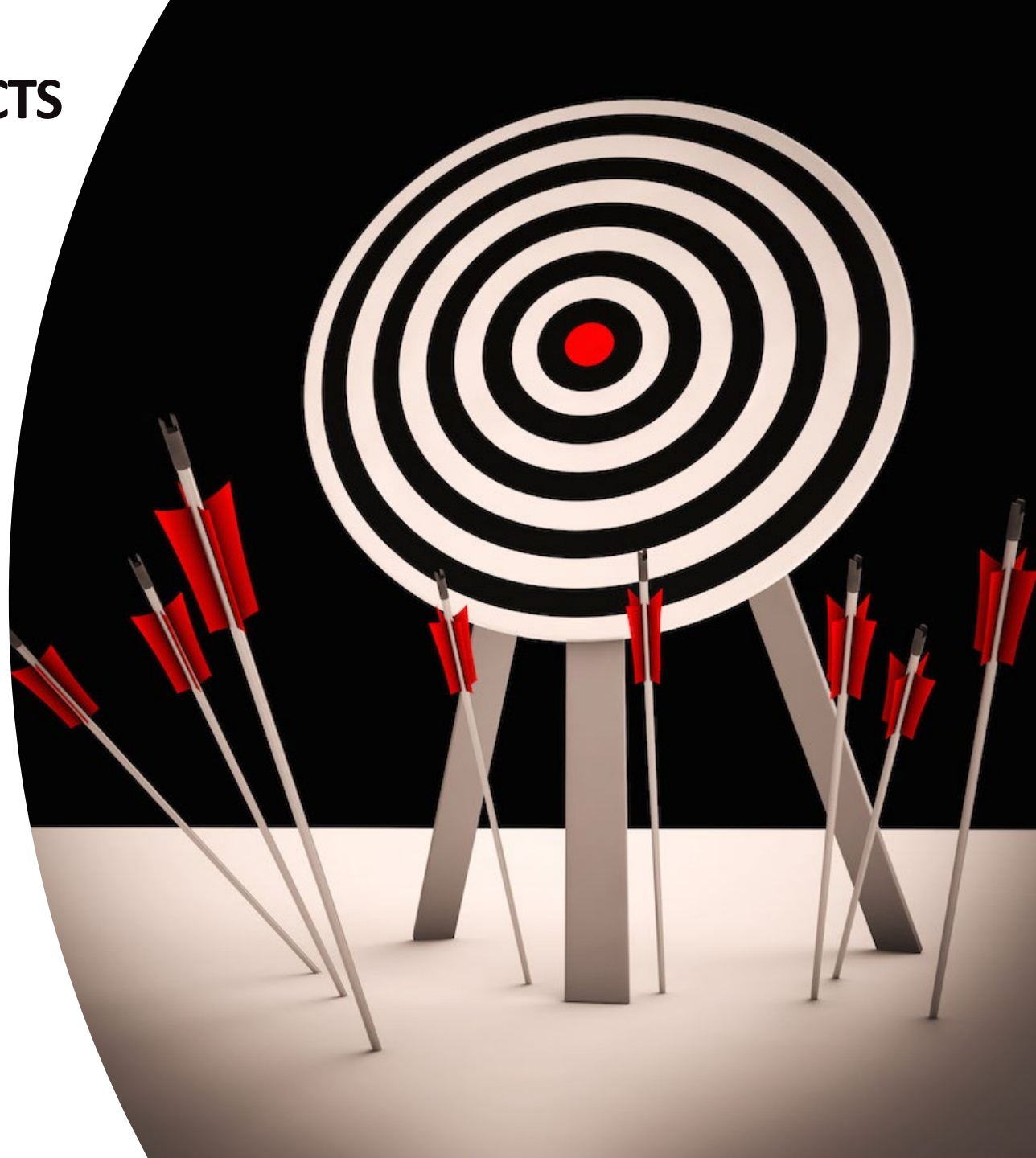
- IoT security is still in its infancy
  - Few devices have been designed with Cyber Security in mind.
  - Even fewer have had any independent cyber security testing

Many people are afraid of what cyber security risks can exist in a device

Others may never give it a second thought until something bad happens

CONNECTED HVAC PRODUCTS SECURITY CHALLENGES

- While a few emerging standards for security do exist, they still fall well short of the mark
  - Many existing standards only look at the device in isolation
    - Many IoT devices come with a cloud service component that is equally important to secure
  - Others standards do not fully address the impact of IoT device existing systems
    - Could your device be used as a gateway to a client's internal networks



CONNECTED HVAC PRODUCTS SECURITY CHALLENGES

- It is not just about the security of your device
  - Many IoT devices connect to a cloud service
  - The cloud service has privileged access to the devices
  - The cloud services may maintain sensitive client data
  - If the cloud service is offline some or all functionality on all IoT devices can be impacted

- DO YOU HAVE A CLOUD SECURITY PLAN?

CONNECTED HVAC PRODUCTS SECURITY CHALLENGES

- So your IoT device is now installed inside someone's home, business, government office…
  - It has access to the client’s network internal

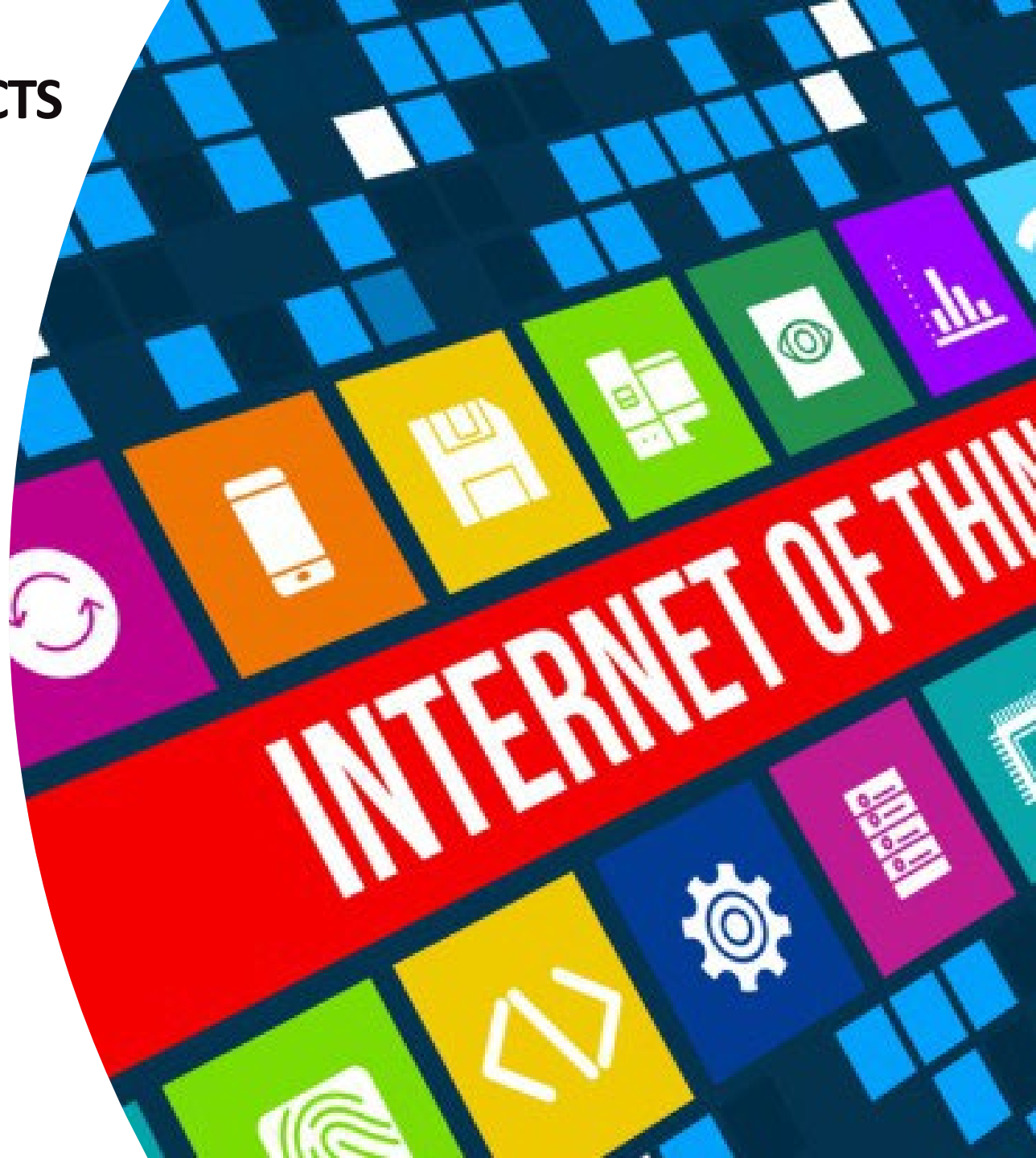
- Why should the client trust you to have privileged access to the internal network?
  - A vulnerability in your product may not just impact the operations of your product but could become a weakness to the entire clients network.

CONNECTED HVAC PRODUCTS SECURITY CHALLENGES

- No two IoT devices are the same…
  - Some devices only connect to cell phone apps and others are standalone Internet devices.
  - Some are lightbulbs, some are medical devices, etc…
  - The security solution has to fit the device, data and service provided (risk management)

CONNECTED HVAC PRODUCTS SECURITY CHALLENGES

- The challenge
  - Ensure end to end security of the IoT device, as well as the cloud services it has access to
  - Ensure that the customer data you have access to is protected and not accessible by your employees or third-parties
  - Ensure the hardware device itself is not creating a backdoor on the customer's internal network
  - Ensure that you can push new firmware updates to your devices and that they will not create new risks previously not considered
  - Convince the customer that they should trust you more than the other guys



intertek ewa canada

05

DEVICE SECURITY STANDARDS / APPROACHES

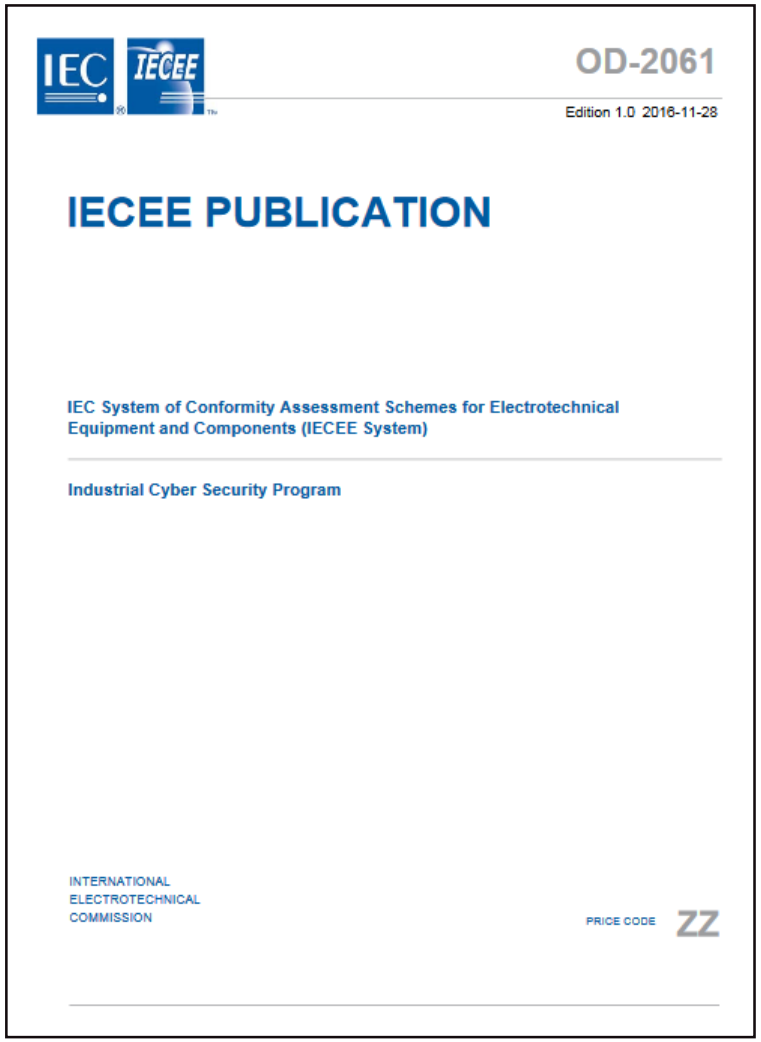
SECURITY STANDARDS / APPROACHES

- **What standard do we pick? (Not a simple answer)**
  - A number of standards currently exists and none of them are yet a clear winner across the board.
    - Likely no single standard will fit everyone's requirements for security.
  - It often depends on the objective of your testing or what your clients are asking for you to provide.

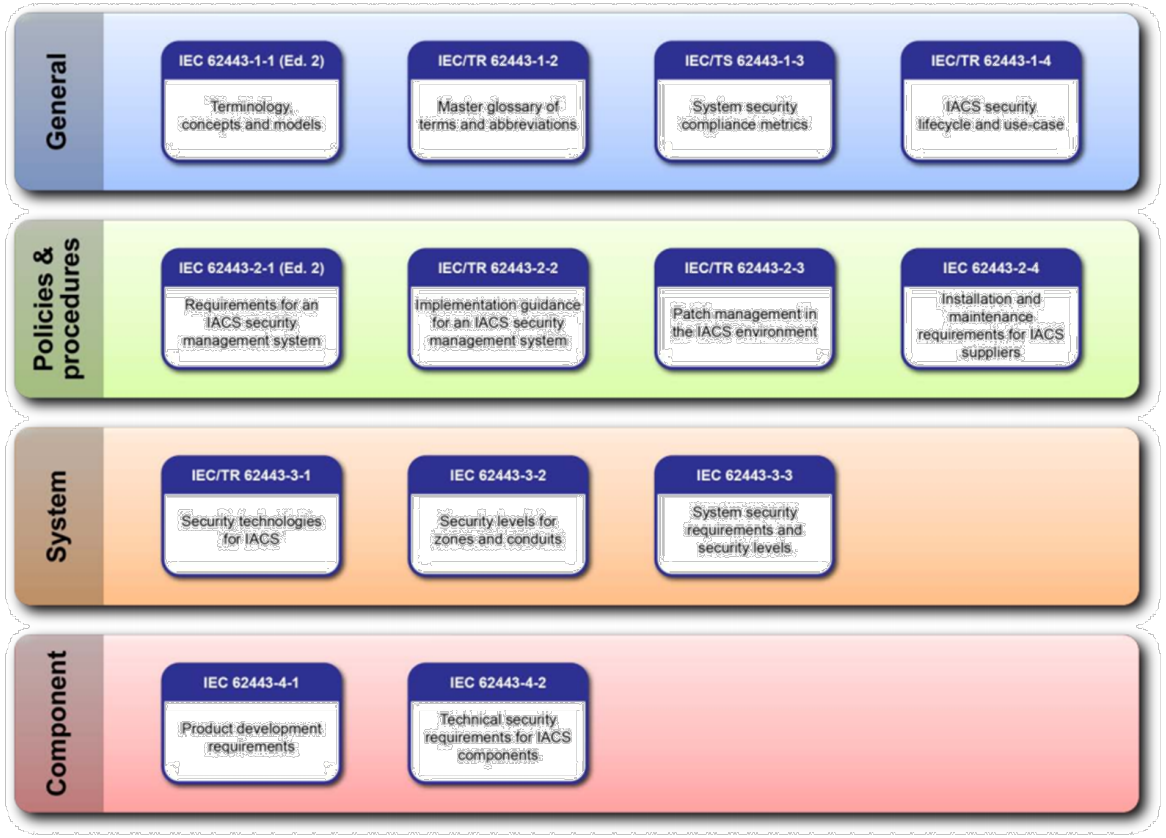
- **Standards, frameworks and regulations, oh my:**
  - IEC 62443 series of standards
  - ANSI/UL 2900 family of standards
  - NIST Framework
  - California IOT Bill

IEC 62443 SERIES

- The IEC has published a conformity assessment scheme for an Industrial Cyber Security Program
  - Intended to provide a framework for assessments of industrial automation controls through a series of standards.
  - An IEC 62443 conformity assessment evaluates:
    - an **applicant's ability to provide** IEC 62443 compliant security capabilities; and
    - that **these capabilities have been applied** to either:
      - a specific product, or
      - a specific solution (an installed product)



STRUCTURE OF THE IEC 62443 SERIES



Source: p. 13 of IEC 62443-3-3 © IEC:2013(E)

Figure 1 – Structure of the IEC 62443 series

INTRODUCTION TO THE ANSI/UL 2900 SERIES OF STANDARDS

What is it?

- *Software Cybersecurity for Network-Connectable Products, Part 1: General Requirements*

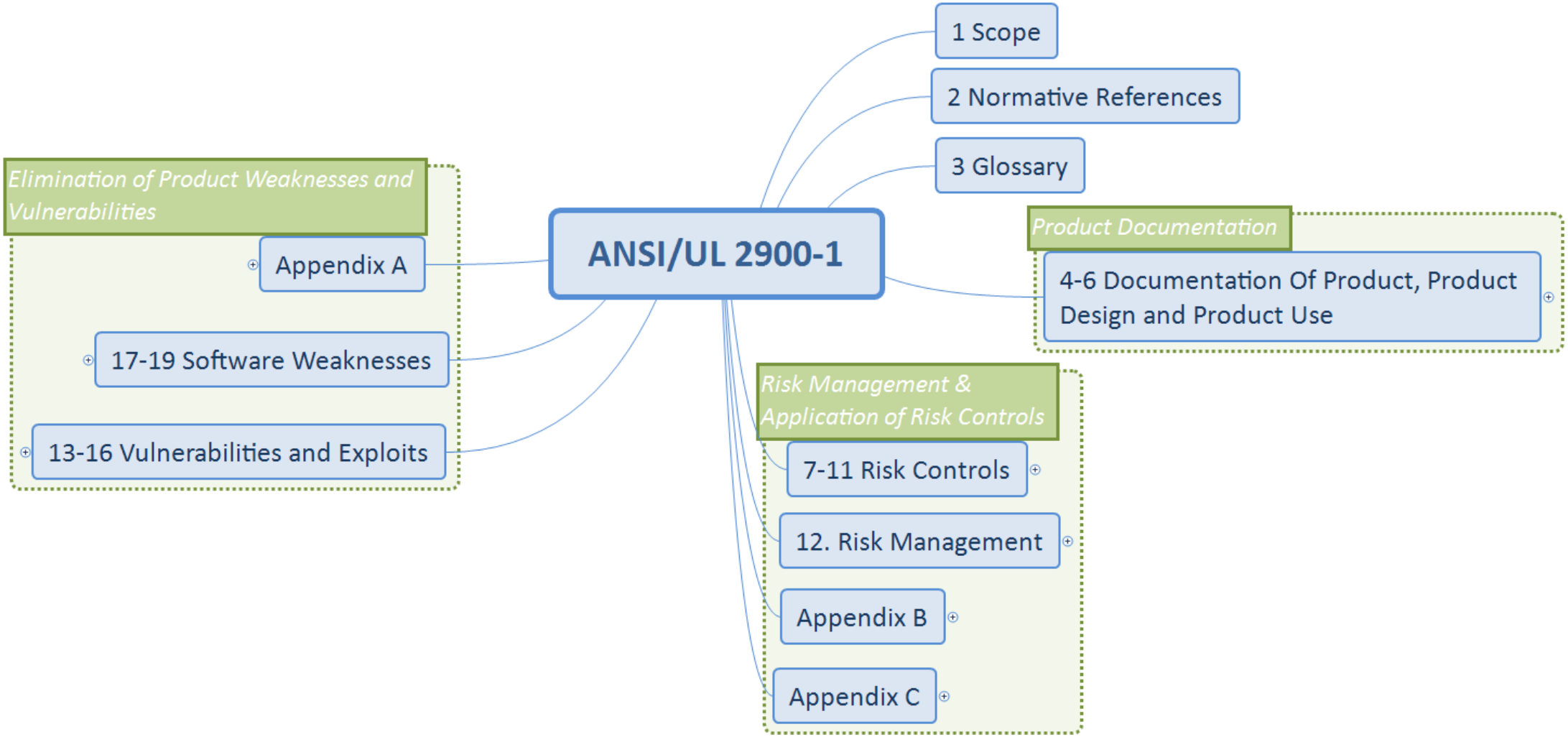
Application?

- Network-connectable products to be evaluated and tested for:
  - vulnerabilities
  - software weaknesses
  - malware

Companion Standards?

- **ANSI/UL 2900-2-1** (Network Connectable Components of Healthcare and Wellness Systems)
- **UL 2900-2-2** (Industrial Control Systems)
- **UL 2900-2-3** (Security and Life Safety Signaling Systems)

ANSI / UL 2900 KEY POINTS



NIST CYBERSECURITY FRAMEWORK

- Published in February 2014 (v1.0) and updated in April 2018 (1.1).
- The Framework provides voluntary guidance, based on existing industry standards, guidelines, and practices.
- The goal is to help organizations manage and reduce cybersecurity risks.
- The Framework only provides guidance and not a checklist of requirements. It must be customized by each organizations to best suit their risks, situations, and needs.
- It is therefore not a standard but an approach for addressing cybersecurity risks.

CALIFORNIA IOT BILL

- Approved by Governor September 28, 2018
- Takes effect January 1, 2020
- Will require a manufacturer of a connected device:
  - to equip the device with a reasonable security feature or features that are appropriate to the nature and function of the device, appropriate to the information it may collect, contain, or transmit, and designed to protect the device and any information contained therein from unauthorized access, destruction, use, modification, or disclosure, as specified.
- This will require you demonstrate reasonable security to protect data:
  - contained in the device (ensure encrypted in storage) ;
  - in transit (ensure encrypted when sent over the wire or wireless outside the device);
  - when store in back end services (ensure encryption of data in storage within cloud services);
  - all copies of client data is deleted upon termination of device or service;
  - ensure access to client data is protected from modification, disclosure.

06

HOW WE HELP CLIENTS

HOW WE HELP CLIENTS…

HELPING PROJECT TEAMS UNDERSTAND SECURITY…

- If a client is still developing a product they should have defined all the security requirements for the product.
- If they haven't, we can help them start to think about what types of threats might exist to the product and vulnerabilities that might reside in the product.
- At this point, we can consider what safeguards (controls) should be implemented

HOW WE HELP CLIENTS…

BAKING SECURITY INTO THE DESIGN…

- Adding security after the fact always costs more…
- The design should be built to be intrinsically secure.
- It should consider the security risks for all services.
  - For example: Locking a door with Google Home or an Amazon Alexa is a lower security action than unlocking the same door.

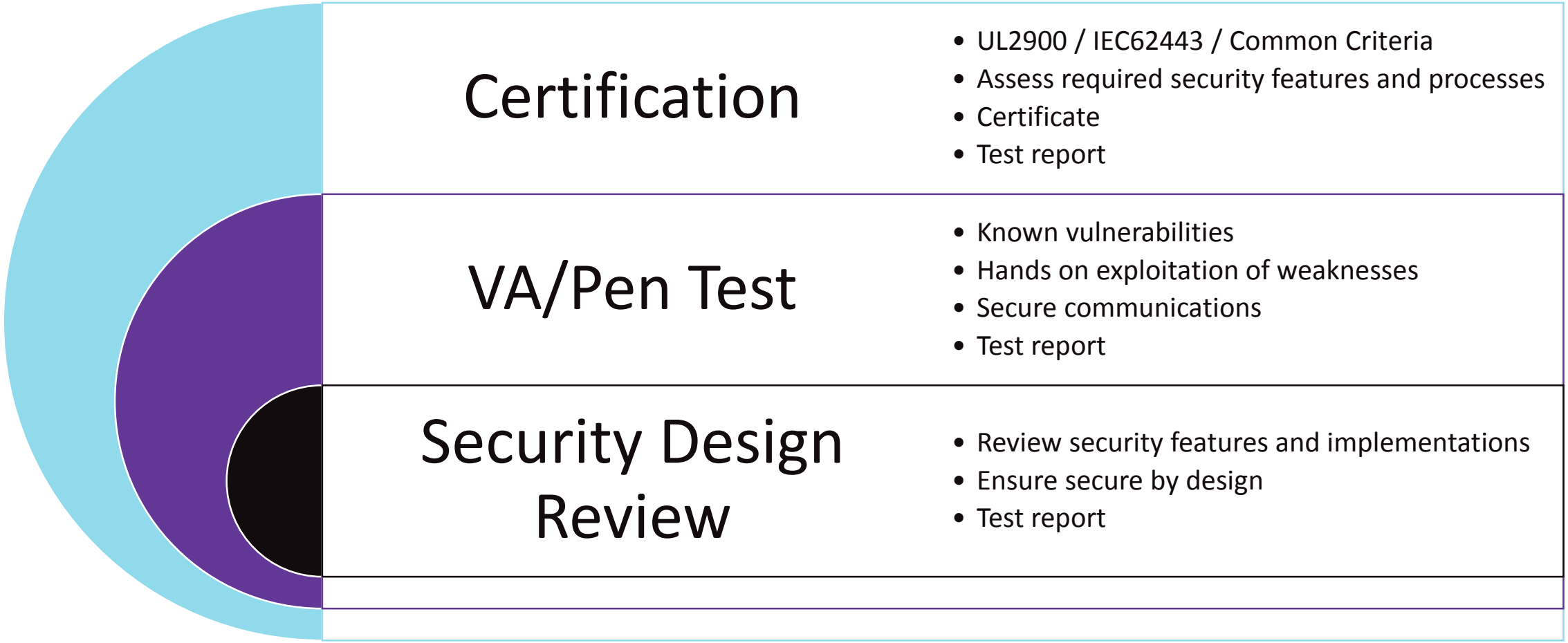
https://teespring.com/shop/the-s-in-iot#pid=369&cid=6513&sid=front

HOW WE HELP CLIENTS…

TESTING ALONG THE DEVELOPMENT PROCESS… (AN ITERATIVE PROCESS)

- If you load all your security testing at the end of a project and everything is fine you're probably lucky.
- If it fails and you find you have a fundamental design flaw, you may have to redesign significant components or start over from scratch.
- For this reason, whenever possible, test your security early and often to ensure you're not making any fundamental mistakes along the way.

SERVICES AND APPROACHES WE CAN PROVIDE TODAY



JOE DAWSON

Principal Software Security Analyst

+1 613 230 6067 ext 1380

joe.dawson@intertek.com

intertek

Total Quality. Assured.