RSAConference2019
San Francisco | March 4–8 | Moscone Center

SESSION ID: **STR-R09**

Getting Product Cybersecurity Right in a Large Mature Corporation

Matthew Bohne

VP & Chief Product Security Officer
Honeywell Building Technologies (HBT)

Cycling… on ice.

What is Product Cybersecurity?

Practice of securing the products & services a company makes.

Works with developers to;

- Design security & privacy features inside of products
- Ensure security and privacy of customer & company
- Manage risks & vulnerabilities across the product portfolio

Responsible for Secure SDLC, policy, technology, IR, testing & training

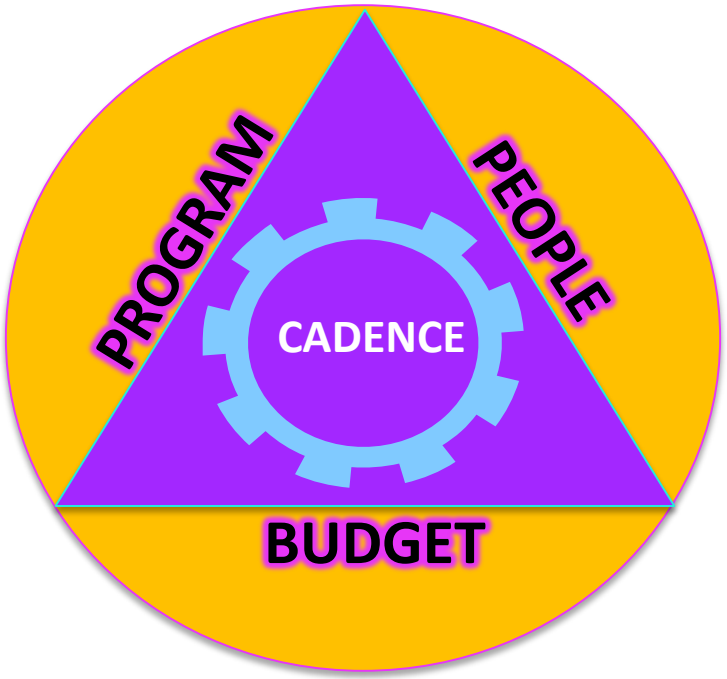
Common Questions …

- What are the big challenges?
- How can I determine what I need (People/ $$s) ?
- What should I do 1st? 2nd?
- What standards & practices should I look to?
- What are best practices for software development lifecycle?
- Budgeting & Funding techniques that can help with this?
- What kind of culture do I need to establish?

Biggest challenges for Product Cyber Leaders

Three of the greatest (perennial) challenges with this space:

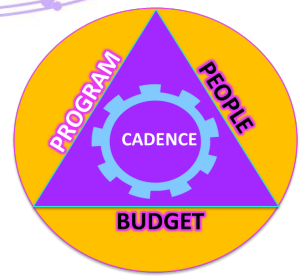
1) **Program** – Strategy, methods & leadership support
2) **Budget** – Million dollar problem w 100k budget
3) **People** – Org imbalance, freeze, behaviors, recruiting

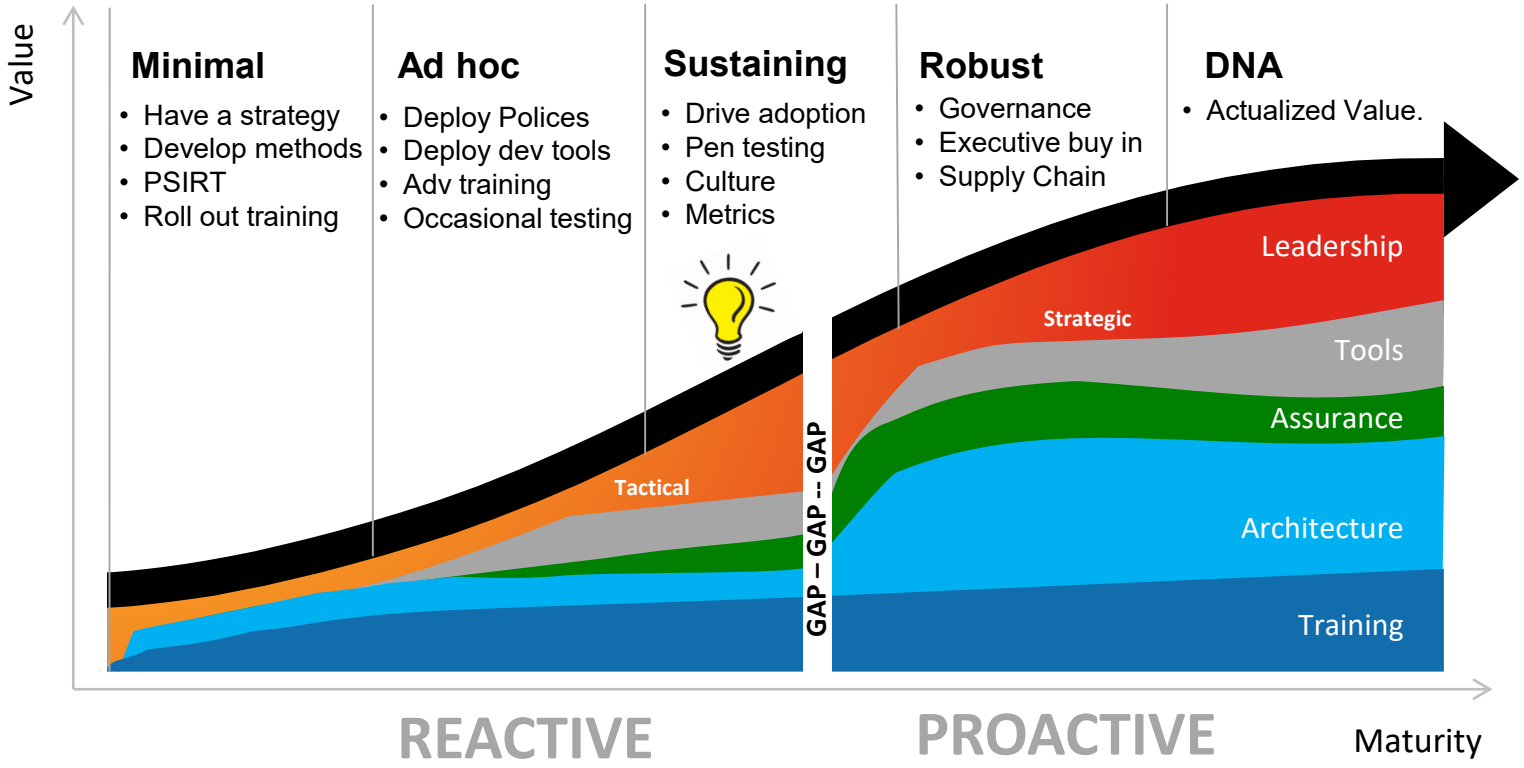


As you overcome 1,2 & 3…

Must stay conscious of cadence for TRACTION

Where is YOUR company?





Challenges:

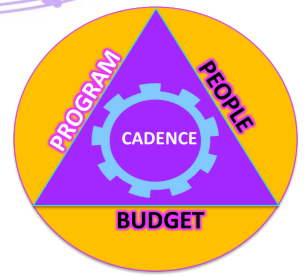
- Location, location, location
- Fixed $ vs needs based
- Champion(s)
- Leadership

Bridging GAP Requires:
- **Executive Support**
- **Financial Support**
- **Competent Staff**

Need a baseline in order to move forward

Tools to help you assess where you are

BSIMM – Building Security In Maturity Model



- Benchmark yourself against 120 others
- 116 controls organized by maturity
- Clear and easy to use
- Start w/ self assess, then 3rd party
- Will help you prioritize actions
- Will help you understand your NEEDS

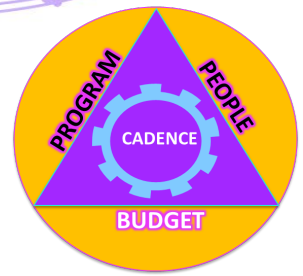
VS

Adobe, Google, SAP, VISA, AON, FannieMae, SallieMae, vmware, Bank of America, Intel, scrippsnetworks, Intuit, WELLS FARGO, McKESSON, Sony Ericsson, CapitalOne, zynga, Microsoft, Symantec, THOMSON REUTERS, DTCC, NOKIA, Fidelity, The Depository Trust & Clearing Corporation, QUALCOMM, SWIFT, EMC², STANDARD LIFE, TELECOM ITALIA, + Many Others.., cigital

The Software Security Framework

Governance	Intelligence	SSDLC	Deployment
Strategy & Metrics	Threat Models	Architecture Analysis	Penetration Testing
Compliance & Policy	Security Features	Code Reviews	Software Environment
Training	Standards & Requirements	Security Testing	Config & Vuln Management

Getting to where YOU need to be



If 50% of companies do this activity why aren't **YOU**?

Cyber Staff to Developers

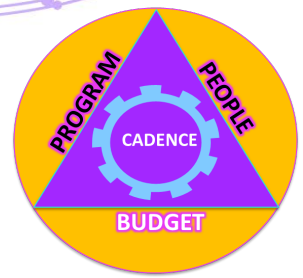
Bridging GAP Requires

- Executive Support
- Financial Support
- Competent Staff

Architects & Assurance Staff to Projects

It's a journey… and it requires skilled people to navigate it

Options to help with Funding

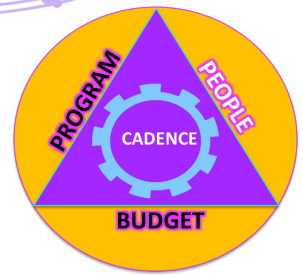


- **KNOW the needs -** start w/ release train owners / Dev managers
- Grow / Fund by products (Similar to QA or HFE) Use RATIOS!
- Several models - start w/ what already resonates
- **Blended budget -** central budget for Assurance… Archs funded out of BU.

Going from 0 to anything is ALWAYS the hardest …Negotiate

Team sport - Get HR, Legal & Finance to help support your case!

Functional Org Example



CEO

VP Eng or Product Development

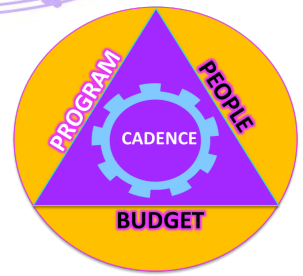
Chief Product Security Officer

Order of Org

Product Security Leaders (2)	Security Architecture (1)	Security Assurance (1)	Security Excellence (2)	Security Enablement (2)	Security Engineering (3)	Governance & Privacy (2)	Incident Management (1)	Supply Chain (3)
Influence	Secure by default	Hunt & detect	Learn, train & validate	Measure & Forecast	Tech to protect	Governance	Communicate	Cyber Export
Evangelists -SBU Oversight -Educate -Lead leaders -CTO signoff -Participates w/ stds bodies	**Security Architects** -Lead security design -Consult on New -Review designs -1 on 1 Educate -Cyber quality -Participates w/ stds bodies	**Cyber Testing** -Penetration -Fuzzing -Physical cyber -Soft/Firmware	**Training & Audit** -Facilitates Standards to Command Media -Build / run training -Assess compliance -Manage WIKI -Plan & Arch training -Audit to train -External Audit interface	**Analytics & Automation** -Cyber reporting & Instrumentation -Compliance reporting -Long term remediation monitoring -CEO/CTO Dashboards	**Cyber Tech** -Cyber Tools -Shared libs -Common reuse -Shared boot -Firmware -PKI code	**Gov & Privacy** - Risk Management -Privacy Req'mnts - GDPR (Product) - Compliance -Participates w/ stds bodies	**PSIRT** -Incident POC -Liaise w/ biz functions -Inventory Mgmt -Escalation Mgmt -Privacy Escalation -Liaise w/ CERTs	**Supply Chain Cyber** - Program & partners - Contract & MSA - External education - Assessments - OEM / ODM Requirements

Don't have to report into one – some can matrix

Product Incident Response Team (PSIRT)



If you make software you <u>should</u> have a PSIRT

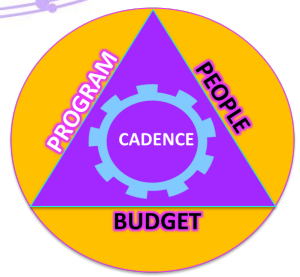
- Have a documented & practiced Incident Response plan
- Many examples: First.org, CERT, ISO & NIST

GREAT: First.org PSIRT Framework + CVSS & CWSS scoring

Still see too many companies without a basic IR/PSIRT

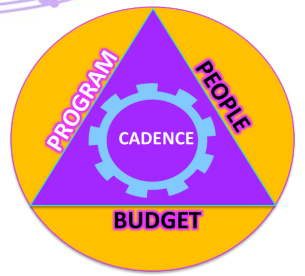
Training

Thoughtful & RELEVANT



- Not the same as IT Security training (ex. USB Policy)
- UNDERSTAND your AUDIENCE – different msgs needed
  - **Executive to Manager** – Awareness & STEWARDSHIP
    - **Developer** (intro to adv controls for specific languages)
    - **Every Employee** – Awareness & their role
    - **Sales/Service** – Cyber capabilities of products
  - **Supplier** – Cyber requirements, PSIRT, Responsibilities
- Bring in CBT vendor for basic SSDLC + secure coding
- Audit to Train

Standards & CERTS



In the absence of practices/ Standards use the following:

- **IOT/IIOT** = ISA/IEC 62443 , (DRAFT) NIST IOT Baseline
- **Cloud** = CSA STAR, SOC 2 Type 2.
- **Product or Process Certifications** = ISASecure, UL 29001
- **People** = CSSLP, Ethical Hacker, CCSK, CCSP, CISSP
  + ISA/IEC 62443 Cybersecurity certificates

- **SSDL** = Microsoft Security Development Lifecycle

Use the right tool for the exercise

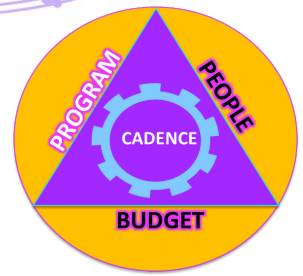
Example: Secure Software Development Lifecycle

Start	Requirements	Design	Development	Testing	Deployment	Maintenance & EOL
Involve Security Architect	Security / Privacy Requirements	Threat Model	Threat Model	Security Tests	Security Review Checklist	"Wash/Repeat" SSDL
	Security Review Checklist	Security Tests	Security /Privacy Requirements	Security Risks	Security Risks	Revise PIA/DPIA
		Security Review Checklist	Security Manual		PIA/DPIA Review	Revise Threat Model
		Security/Privacy Requirements			SIGN OFF	Cust Comms & PSIRT
	Security Risks	Security Risks	Privacy Impact Assessment (PIA)			

Methodology agnostic – works in Agile & Waterfall

Where the work gets done

...is where the TEAM belongs

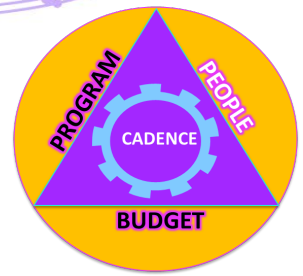


- Where do the software developers report to? **SAME.**
- Product Security is part of Product TCO & ROI (ex. Quality, HFE)
- Fully integrated & blended with development teams
- Product Security different from IT Security
- Collaborate and share (threats/Incidents)

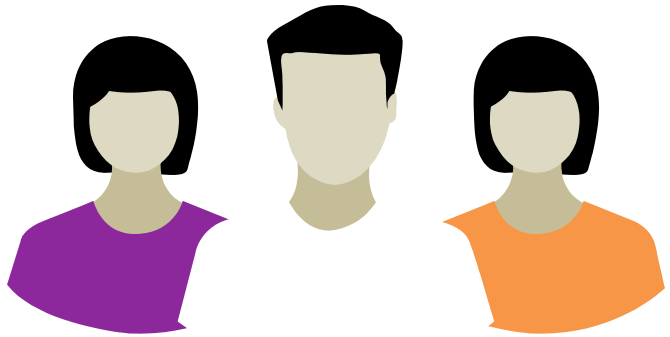
Similar but optimized for different needs…
Mixed results when used for cross purposes

GROWING the TEAM

Its not enough to hire, have to grow literacy



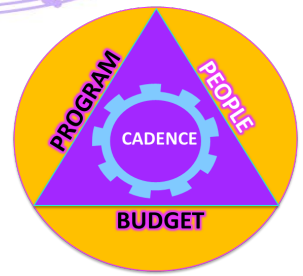
- High demand specialty – Can't win w just $$$
- Train to maintain – logically and regionally
- Passionate Few Program + training
- Fund your team to cyber training & conferences
- Evolve: part time/dotted line to dedicated/solid line
- Build into G&Os and raise the bar annually.
- Certify where it makes sense



This becomes part of the culture YOU build and sustain

Culture

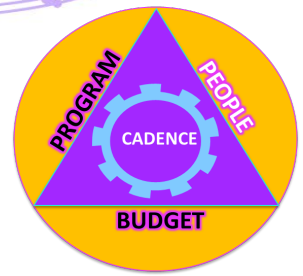
YOU are responsible for the environment



- Trust & Collaboration cornerstone of successful teams
- Arrogance kills collaboration and undermines TRUST
- Inclusive vs Exclusive
- Remember why people leave – don't be that leader
- Respect & reward the tech – teach the behaviors
- Share and give away everything (internal)

Give regular training on communication skills and negotiation!

Leadership



- Who is your executive champion(s)?
- Build the story and sell the story to peers and executives
- KNOW BUSINESS's DATES and be EARLY (Budget, Quarterlies etc)
- BUILD important relationships with FINANCE, LEGAL, HR and SALES
- Make sure you and HR on same page (ex. salary, recruiting)
- Understand your own weaknesses – grow and bring in stronger
- Clarity is more important than perfection

Cyber is a team sport

you need EVERYONE to do their part

Executive Team

Ex. Stewardship, Company msg & posture

Marketing / Comms

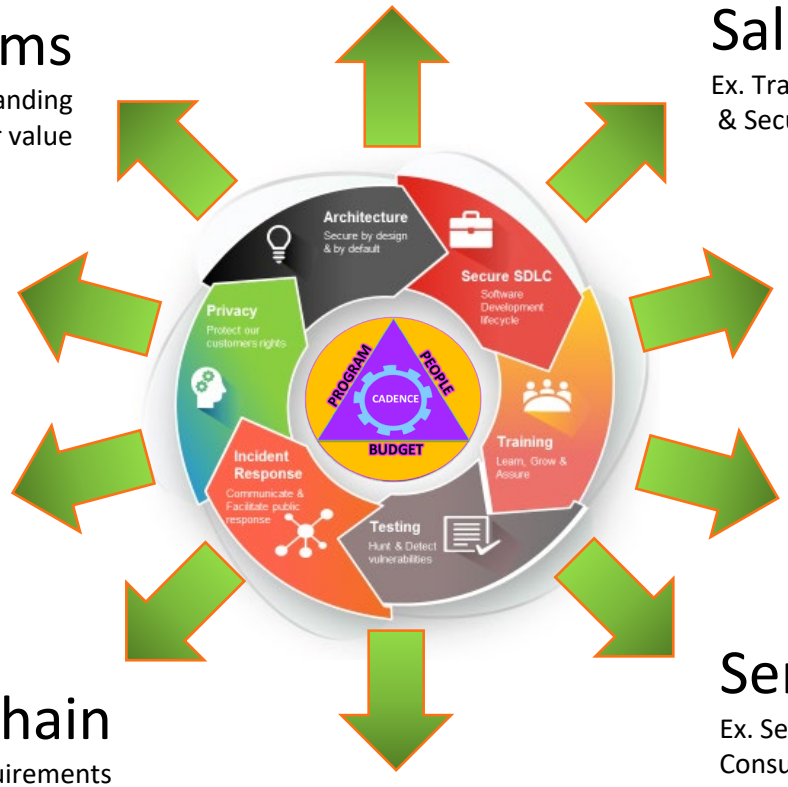
Ex. PSIRT, cyber branding
Knowledge of cyber value

Sales

Ex. Trained in cyber value to customer
& Security features in product

BD/M&A

Ex. M&A Cyber Assessments



Engineering

Ex. Secure development, BUILDS Security & Privacy features
Remote upgrade & patch management

Legal

Ex. T&Cs, Regulation
Privacy & PSIRT

Manufacture (incl OEM & ODM)

Ex. PKI, Secure boot

Supply Chain

Ex. T&Cs, disclosure requirements
Secure by design & privacy

Service

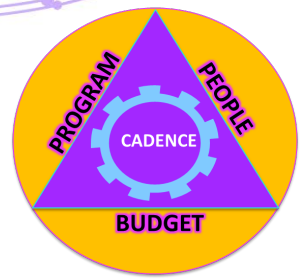
Ex. Secure Installation & Configuration and MAINTAIN…
Consult to customer on security

IT

Ex. IP protection, Internal &
Employee Privacy.

Having a strong executive champion is a key success factor

Applying What You've Learned Today



Next week you should:

- Assess where you are in relation to what you've learned (Knowledge/$/People)
- Identify your roadblocks (Program? Budget? Structural?)
- Identify your key stakeholders/Champions you need to influence

In the first three months following this presentation you should:

- Self assess (ex. BSIMM) & Identify key areas of improvement
- What's your "story" to make improvements & correct / overcome roadblocks (ex. Structure)
- Build/reinforce relationships with your TEAM & Champion(s) – INVEST NOW

Within six months you should:

- Budget defined and BROADLY shared (& bought into) w/ ALL stakeholders
- Report out to your leadership w CLEAR & SIMPLE plan (ex. MGPP) to enhance your program