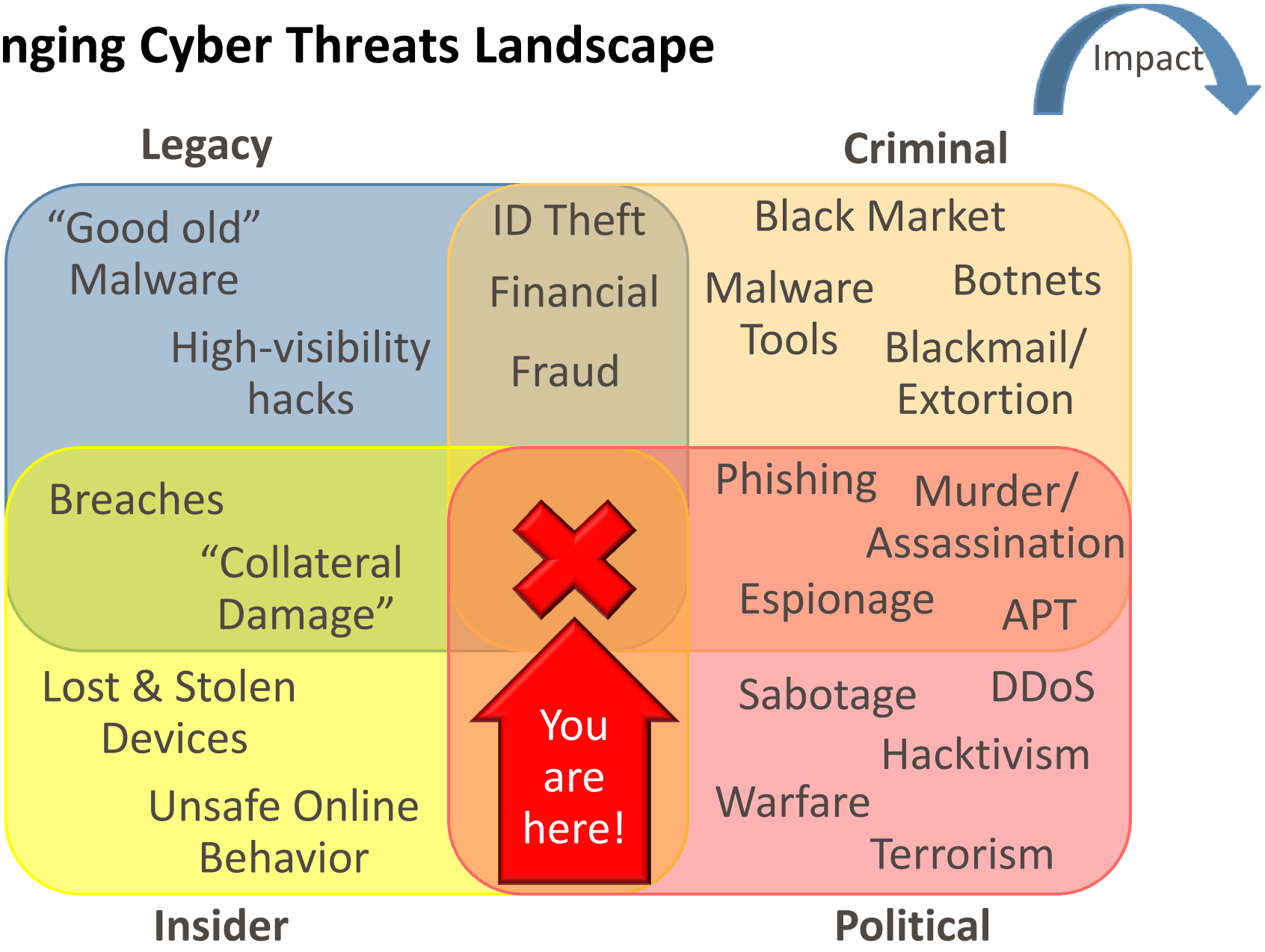
Surveillance and Forensics for Cybersecurity-associated Device Risks

Axel Wirth, CPHIMS, CISSP, HCISPP

Healthcare Solutions Architect,
Distinguished Systems Engineer
Symantec Healthcare Industry

September 10th, 2014

Changing Cyber Threats Landscape



Why is Medical Device Cybersecurity a problem? And why now?

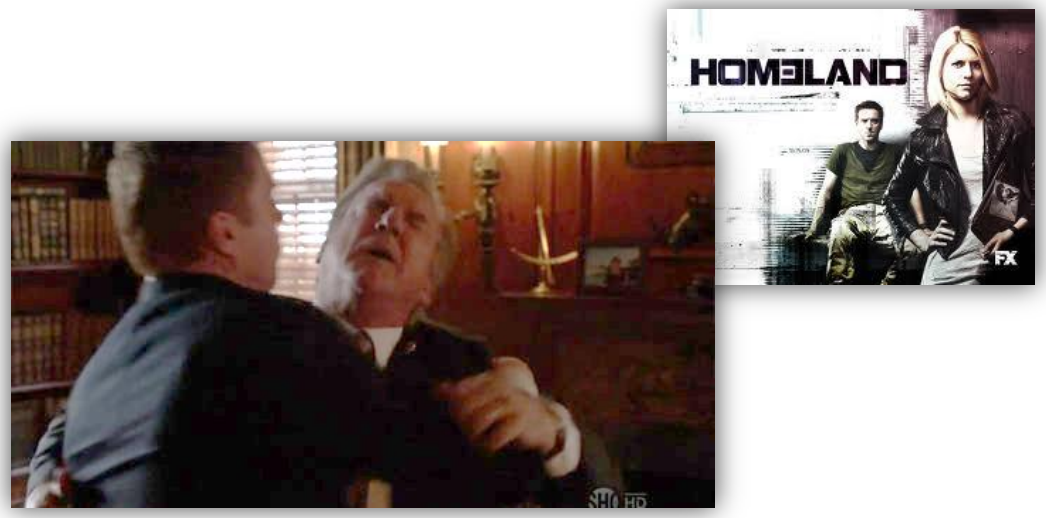
Risk:
- Patient safety (lives)
- Operational / Downtime
- Data Breach
- Revenue / Financial
- Patient trust & staff morale

Threats:
- Targeted attacks
- Collateral damage
- Malware remediation
- Theft / Loss
- Compliance violation
- National security; terrorism

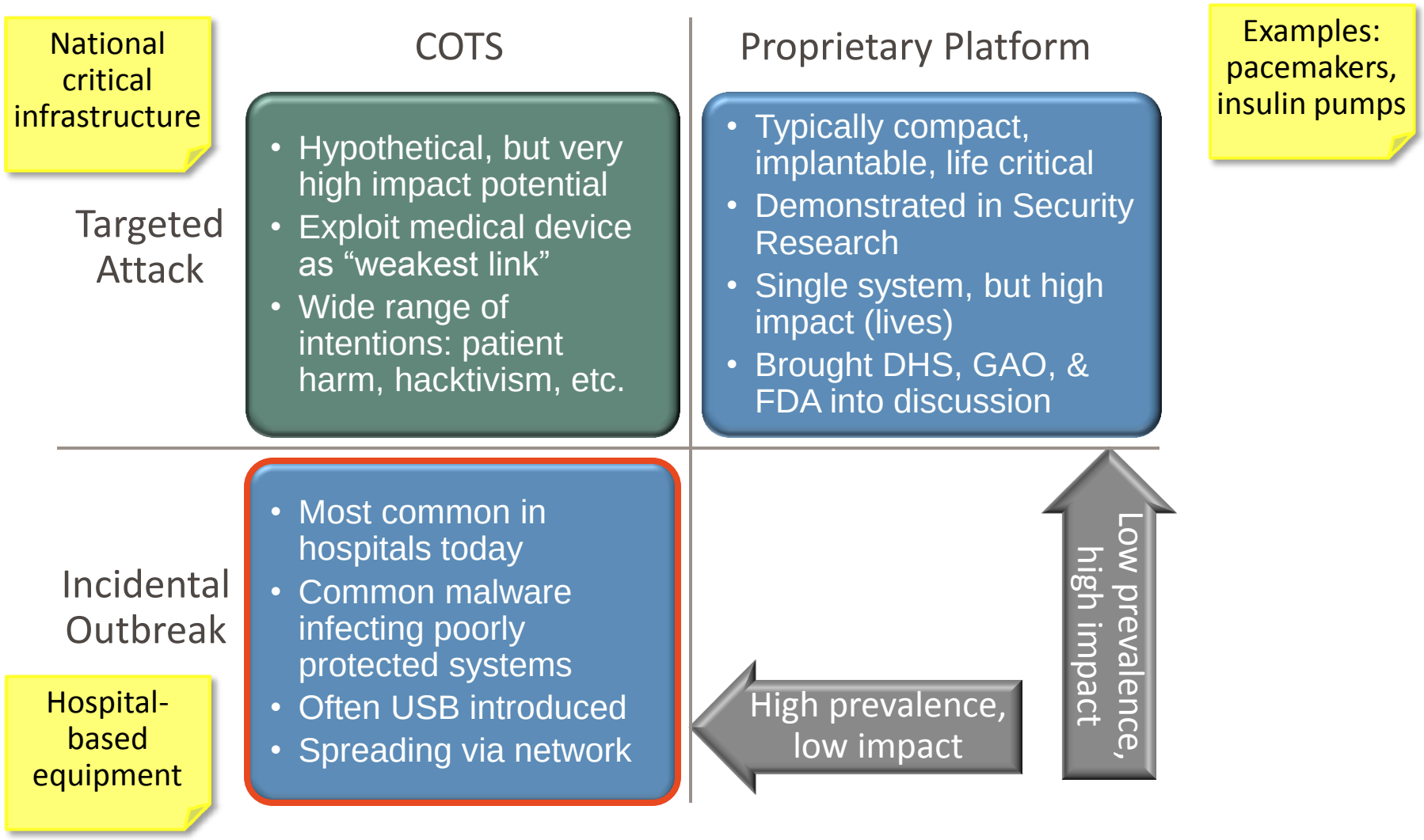
Vulnerability:
- Highly regulated (FDA, HIPAA)
- Long useful life
- Poorly protected & patched
- Vulnerability of device, hospital, & health system
- "Weakest link"
- Complexity

A Brief Timeline of Medical Device Security

2008	2009	2010	2011	2012	2013	2014
"Pacemaker hack" UMass Amherst (Kevin Fu)	Conficker infects Med Cabinets, nurses to manually deliver meds for 24 hrs.	More reports from customers, e.g. outbreak requiring diversion of all cardiac emergencies.	"Insulin Pump hack" (Jerome Radcliffe)	GAO report: "FDA Should Expand Its Consideration of Information Security for Certain Device Types".	FDA guidance for manufacturers and healthcare providers; Homeland Security ICS-CERT cyber security alert.	• Increasing manufacturer security focus • NCCoE project • Device security testing • AAMI/ECRI "Top 5 Hazards"



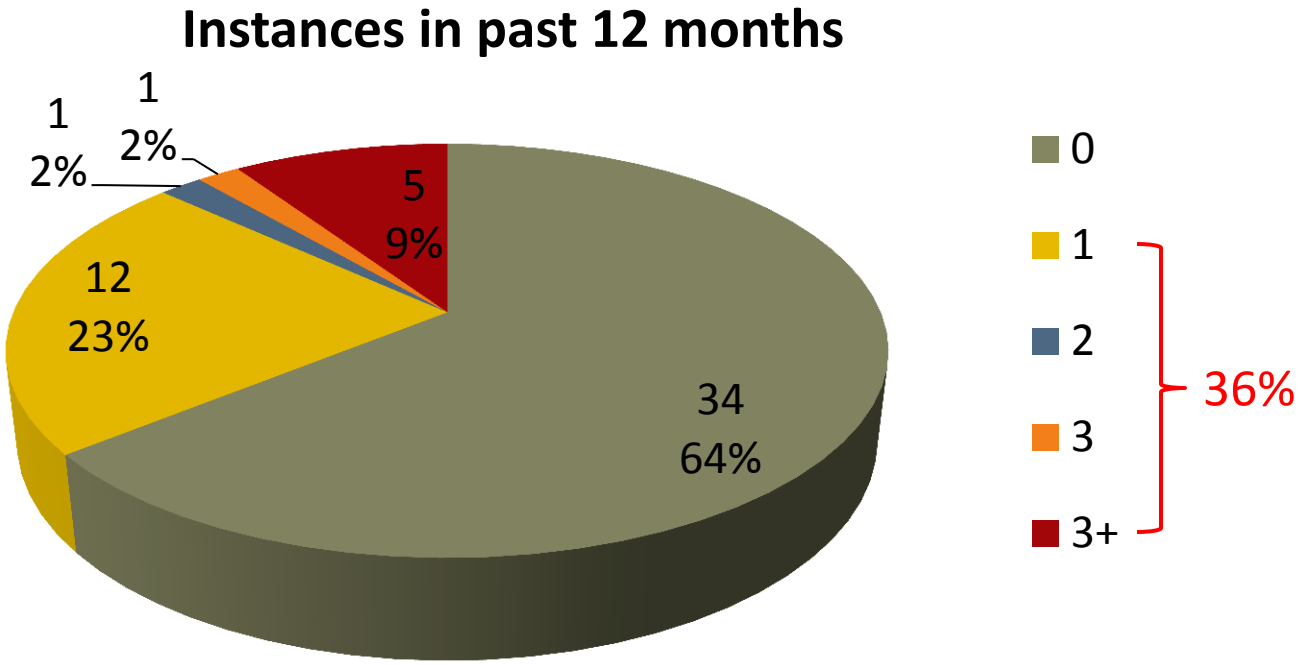
Infection Scenarios: Intentional vs. Unintentional



COTS = Commercial off-the-shelf Software

CHIME Med Device Security Survey – Key Findings

Q9: How many, if any, instance(s) of a virus or malware outbreak specific to a medical device occurred within your institution in the past 12 months?



Takeaway: 36% have had one or more instances, with 13% reporting multiple instances. (Q10: 17% saw an increase over the previous period).

http://www.symantec.com/content/en/us/enterprise/white_papers/b-networked_medical_devices_WP_21177186.en-us.pdf

Surveillance and Forensics – Status Quo

- To date, no systematic collection and analysis of medical device vulnerabilities and incidents exists!
- Ample of anecdotal evidence:
  - Security research (pacemaker, insulin pump)
  - Examples of “collateral damage” incidents via network, USB:
    - Shut down automated medication delivery for 24 hrs.
    - Diversion of cardiac emergencies due to interventional Cardiology shutdown (all systems)
    - Data breach through stolen Ultrasound scanner
    - Reports of hospitals testing “samples” of devices or performing device network penetration testing
- Piecemeal examples:
  - FDA MAUDE DB, FDA Cybersecurity Lab, Symantec survey, Philips Disclosure Policy

Surveillance and Forensics – Status Quo

- What we could do if …. :
  - Articulate scope of the problem
  - Assess operational and financial impact
  - Technical analysis (malware, attack, exploit, etc.)
  - Analyze infection mechanism
- As a result:
  - Set the right priorities
  - Focus on the largest impact solutions
  - Justify and align investments
  - Improve device design and integration
  - Educate all stakeholders; support the right decisions
  - Improve workflows and device handling
  - End the discussion on whether this is a problem once and for all times …..

Thank you!

Axel Wirth

axel_wirth@symantec.com (617) 999 4035