

Building Trustworthy eHealth Applications

Ben Kokx

Director Product Security, Philips

2016-11-23

Trends in healthcare require innovative solutions



Consumers increasingly engaged in their health



Shift to **value-based healthcare** will reduce waste, increase access and improve outcomes



Care shifting to **lower cost settings** and homes




*Connectivity and digital shifting value from devices to **software and services***



Increased connectivity

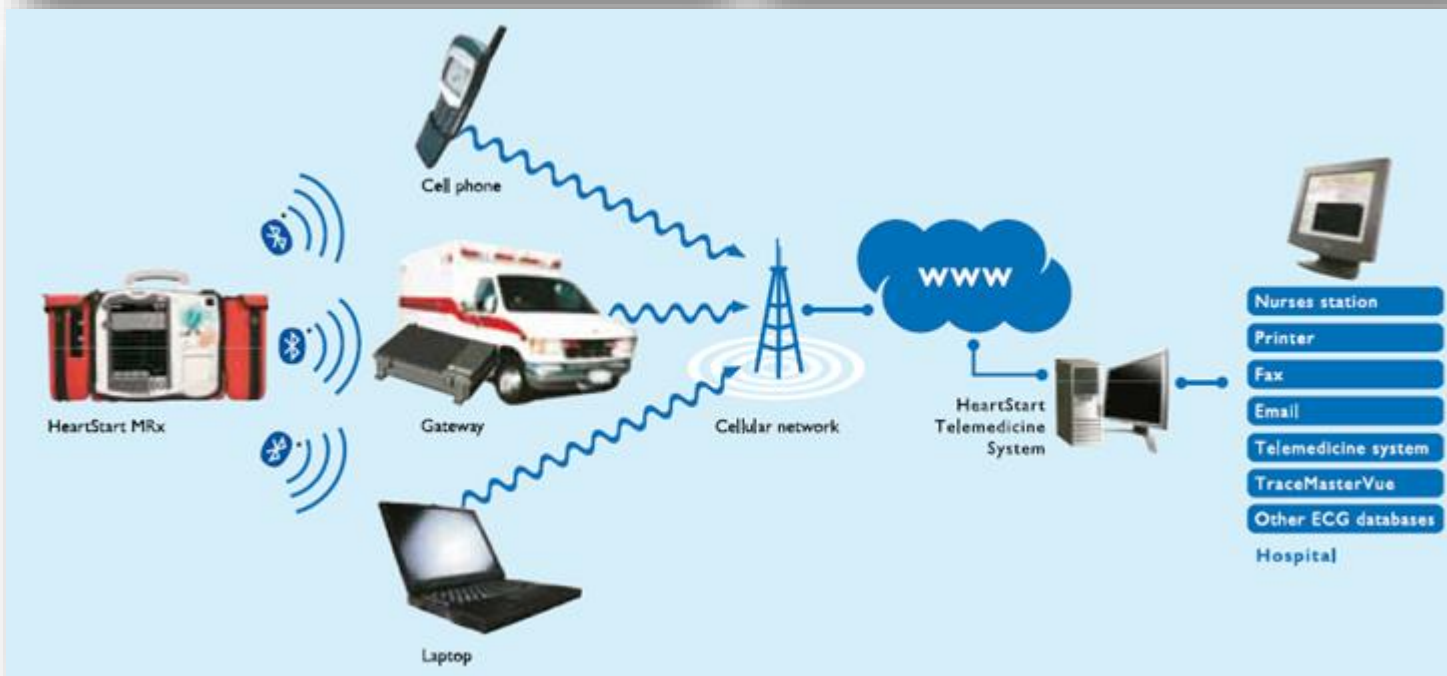
Safety Philips Lifeline Medical Alert Service



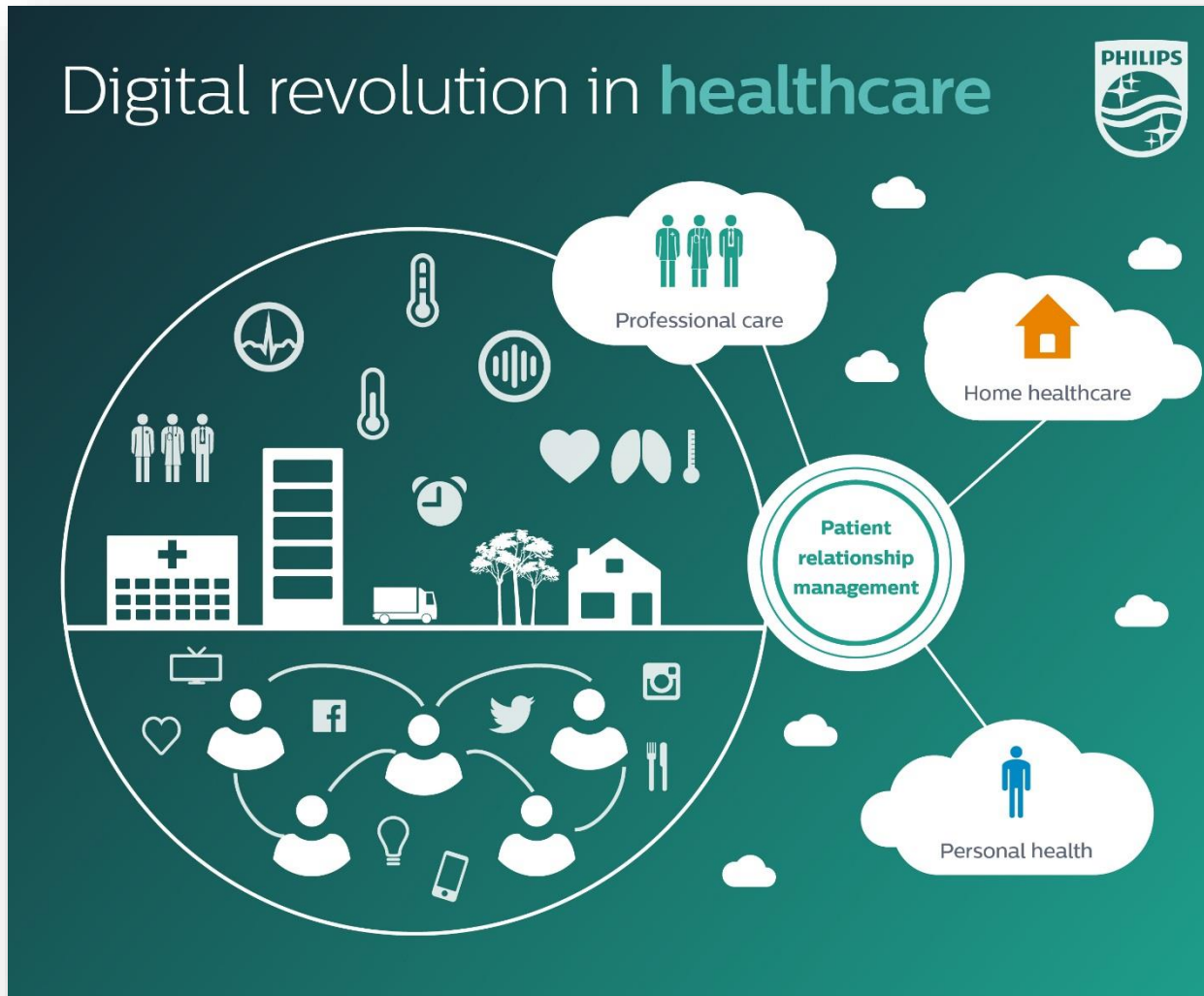
On the Go:
GoSafe

At Home:
HomeSafe

On Your Phone:
Response App



Transformation brings challenges



- New technology
- Increasing complexity
- Big data collections
- Interconnectivity
- Collaboration
 - B2B
 - B2C
 - B2G
- Supply chain risk
- Multiple stakeholders
- Liability



Threat Landscape

Medical world

The Register
Biting the hand that feeds IT

DATA CENTRE SOFTWARE NETWORKS SECURITY INFRASTRUCTURE BUSINESS HARDWARE SCIENCE

Security

Thousands of 'directly hackable' hospital devices exposed online

Hackers make 55,416 logins to MRIs, defibrillator honeypots



29 Sep 2015 at 06:34, Darren Pauli



Derbycon Thousands of critical medical systems – including Magnetic Resonance Imaging machines and nuclear medicine devices – that are vulnerable to attack have been found exposed online.

Security researchers Scott Erven and Mark Collao found, for one example, a "very large" unnamed US healthcare organization exposing more than 68,000 medical systems. That US org has some 12,000 staff and 3,000 physicians.

Exposed were 21 anaesthesia, 488 cardiology, 67 nuclear medical, and 133 infusion systems, 31 pacemakers, 97 MRI scanners, and 323 picture archiving and communications gear.

Los Angeles hospital paid \$17,000 in bitcoin to ransomware hackers

Hollywood Presbyterian Medical Center had [lost access](#) to its computer systems since 5 February after hackers installed a virus that encrypted their files



📍 'The quickest and most efficient way to restore our systems ... was to pay the ransom,' said Allen Stefanek, president and chief executive of Hollywood Presbyterian Medical Center. Photograph: Mario Anzuoni/Reuters

A [Los Angeles](#) hospital hit by ransomware swallowed the bitter pill: it paid off the hackers.

Hollywood Presbyterian Medical Center had [lost access](#) to its computer systems since 5 February after hackers installed a virus that encrypted their computer files. The only out was if the hospital paid the hackers \$17,000 worth of bitcoins, the digital currency.



[Home](#)

[Food](#)

[Drugs](#)

[Medical Devices](#)

[Radiation-Emitting Products](#)

[Vaccines, Blood & Biologics](#)

[Animal & Veterinary](#)

[Cosmetics](#)

[Tobacco Products](#)

Safety

[Home](#) > [Safety](#) > [MedWatch The FDA Safety Information and Adverse Event Reporting Program](#) > [Safety Information](#) > [Safety Alerts for Human Medical Products](#)

Safety Alerts for Human Medical Products

[2015 Safety Alerts for Human Medical Products](#)

[2014 Safety Alerts for Human Medical Products](#)

[2013 Safety Alerts for Human Medical Products](#)

[2012 Safety Alerts for Human Medical Products](#)

Symbiq Infusion System by Hospira: FDA Safety Communication - Cybersecurity Vulnerabilities



SHARE



TWEET



LINKEDIN



PIN IT



EMAIL



PRINT

[Posted 07/31/2015]

AUDIENCE: Risk Manager, Oncology, Nursing

ISSUE: The FDA, the U.S. Department of Homeland Security's Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), and Hospira are aware of cybersecurity vulnerabilities associated with the Symbiq Infusion System. FDA strongly encourages health care facilities transition to alternative infusion systems, and discontinue use of these pumps.

Hospira and an independent researcher confirmed that Hospira's Symbiq Infusion System could be accessed remotely through a hospital's network. This could allow an unauthorized user to control the device and change the dosage the pump delivers, which could lead to over- or under-infusion of critical patient therapies. The FDA and Hospira are currently not aware of any patient adverse events or unauthorized access of a Symbiq Infusion System in a health care setting.



Security researchers

darkREADING
Protect The Business Enable Access

Biting the hand that feeds IT

Get the Dark Reading on security.

SEARCH

Advanced Threats Applications Attacks & Breaches Compliance Database Endpoint Insider Threat Management Mobile
Monitoring Perimeter Risk Security Analytics Services SMB Threat Intel Vuln Management Vulns & Threats More

InformationWeek CONFERENCE @ INTEROP
MAR 31 - APR 1, 2014 Las Vegas, NV
Goodbye IT, Hello Digital Business
REGISTER NOW

NEWS

Security Researchers Expose Bug In Medical System Used With X-Ray Machines, Other Devices

Kelly Jackson Higgins
See more from Kelly | Connect directly with Kelly: [Twitter] [Google+] [RSS] Bio | Contact

ICS-CERT now handling medical device vulnerability alerts in addition to SCADA/ICS vulnerabilities

Start The Discussion | 1 Like | 14 Tweets | 5 Google+ | 2 LinkedIn | Submit | Mail | Print

Kelly Jackson Higgins January 17, 2013
[UPDATED with Philips comments and clarifying that the product interfaces with X-ray machines, but is not an X-ray machine as originally reported.]

MIAMI, FL -- S4 Conference – A pair of researchers best known for poking holes in industrial control systems (ICS) products found that medical devices suffer similar security woes after they were able to easily hack into a Philips medical information management system that directly

Follow Dark Reading
[Facebook] [Twitter] [Google+] [LinkedIn] [RSS] [Email]

Dark Reading Reports

Choosing, Managing and Evaluating a Penetration Testing Service
Pen testing helps companies become more secure by finding and analyzing their insecurities, but pen test services can be fraught with their own kind of risk. In this Dark Reading report, we recommend what to look for in a provider and its wares, how to get what you pay for, and how to ensure that pen testing itself doesn't open the company or its employees up to new risk.

Integrating Vulnerability Management Into the Application Development Process
There's no such thing as perfection when it comes to software applications, but organizations should make every effort to ensure that their developers do everything in their power to get as close as possible. This Dark Reading

The effect of the increased sensitivity for security and privacy (enforced by law)

GDPR, NIS & many others...

- Hospital IT departments are becoming (more) involved in the medical device / medical IT procurement process
- Shift risk to suppliers:
 - Master Security Agreements
- Restricting access to patient data:
 - Limit usage of removable media
 - Limit physical access to patient data
 - Increased pushback on remote access



In control

Major stakeholders

Hospital Administration	<ul style="list-style-type: none">• Efficiency care and cost• Compliance with regulation
Caregiver	<ul style="list-style-type: none">• Best diagnosis, treatment & overall care, fast workflow• Health-affirming and cost-effective outcomes
Patient	<ul style="list-style-type: none">• Treatment, resolution, Prevention• Affordable, Quality, Privacy
Security & Privacy	<ul style="list-style-type: none">• Confidentiality, Integrity & Availability• Transparency
Manufacturer	<ul style="list-style-type: none">• Best-in-class medical systems and healthcare IT• Safety & effectiveness, security, privacy, innovation, value, IP protection & customer satisfaction
Government & Regulator	<ul style="list-style-type: none">• Regulating under law• Safety & effectiveness (starting to include security)• Affordable

Common factors for most incidents

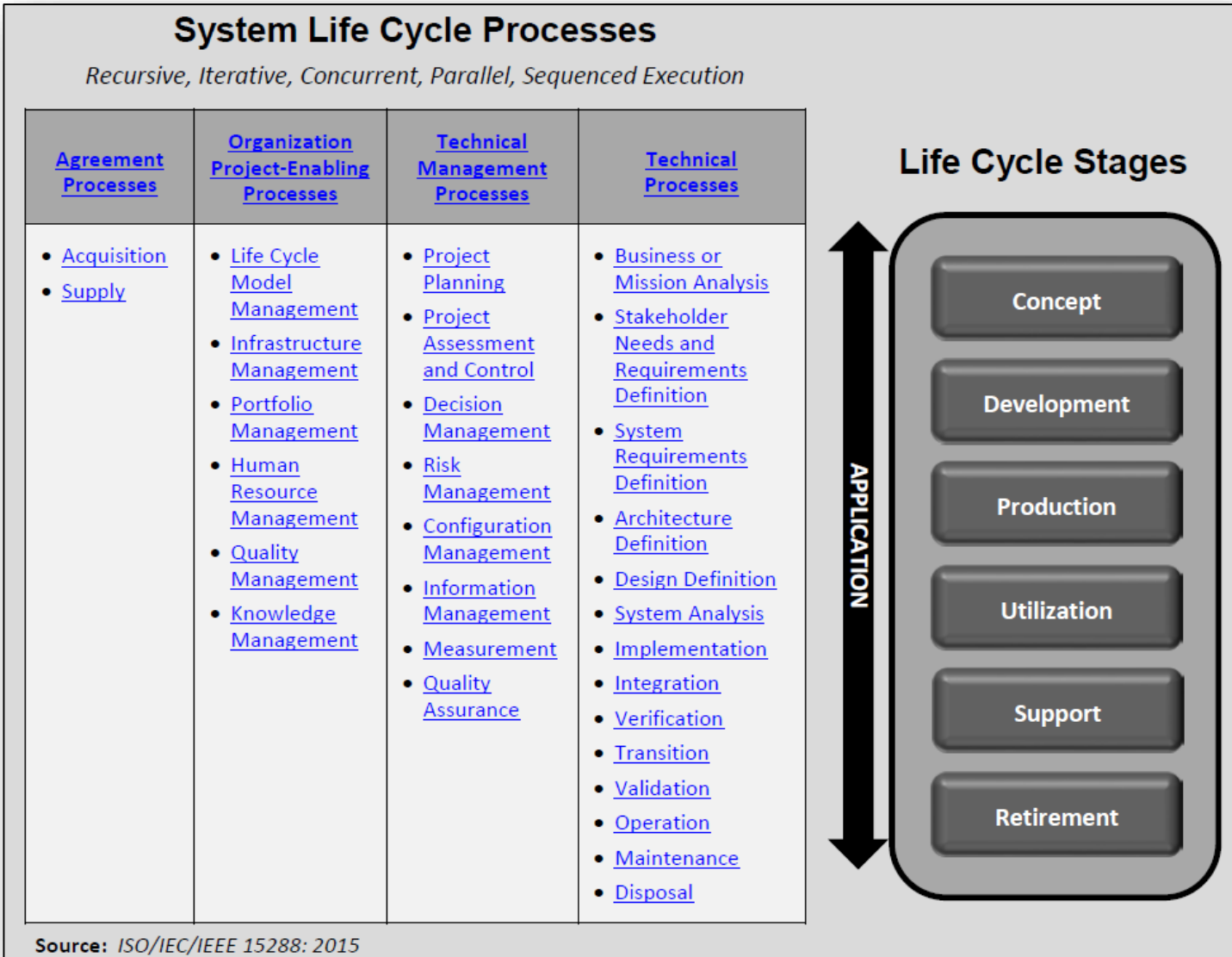


- Forgetting the fundamentals
- Not considering best practices
- No attention to maintenance
- Lack of awareness
- Lack of knowledge
- Lack of attention and focus



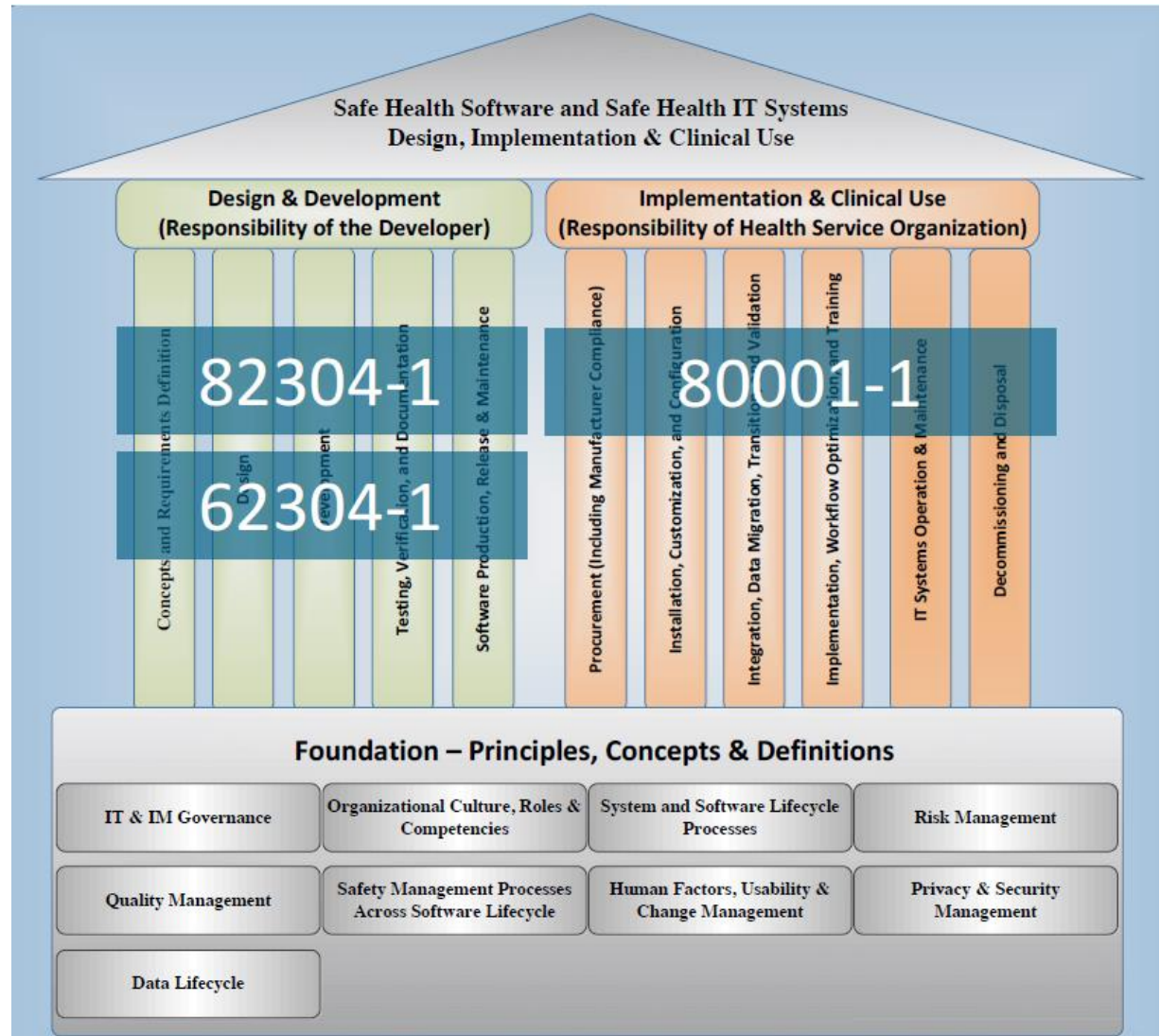
NIST SP800-160 Systems Security Engineering

Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems



ISO/IEC 80001-1:2010 Revision afoot!

- Usability & Lessons Learned
- Focus on Key Properties: Safety, Effectiveness, Security
- Health Software
- 31000 vs. 14971



Many applicable Security Standards

Just a few listed here:

- ISO/IEC 15408; Information technology - Evaluation criteria for IT security
- ISO/IEC 27000 series; Information technology – Security techniques, e.g. 27002 – Code of practice for information security controls
- ISO 27999; Health informatics - Information security management
- IEC 62443; Industrial communication networks - Network and system security
- ISO/IEC 62304; Medical device software - Software life cycle processes
- IEC-80001; Application of risk management for IT Networks incorporating medical devices
- ISO/IEC 29101; Privacy architecture framework
- ISO/IEC 29147; Vulnerability Disclosure
- ISO/IEC 30111; Vulnerability Handling process
- Many applicable NIST standards such as NIST SP 800–33, SP 800-82 and specifically SP 800-53 and the recently released SP 800-160
- AAMI TIR57; Principles for medical device security Risk management

Coordinated Vulnerability Disclosure



Launch of the Coordinated Vulnerability Disclosure Manifesto at the EU high-level Cyber Security meeting on May 12th 2016 in Amsterdam



Coordinated Vulnerability Disclosure Manifesto

Over the last decades, the importance of ICT and the role it plays in our everyday lives has increased exponentially. As our interconnectedness grows and the dependence of our societies on the Internet and ICT increases, the potential negative impact of vulnerabilities in ICT also increases. Consequently, finding and remedying those vulnerabilities is increasingly important.

Cooperation between organizations and the cyber security community can be helpful in finding and fixing vulnerabilities. A mechanism of cooperation that is already used in that regard is *coordinated vulnerability disclosure* or *responsible disclosure*. Essentially, this is a form of cooperation in which vulnerabilities are reported to the owner of the information system, allowing the organization the opportunity to diagnose and remedy the vulnerability before detailed vulnerability information is disclosed to third parties or the public. Further publication will be coordinated between the finder and the organization.

With this manifesto, initiated by Rabobank and CIO-Platform Nederland, the signing parties try to raise awareness for the importance of cooperation between organizations and the ICT-community to find and solve ICT-vulnerabilities. In the experience of the initiators, such cooperation results in many vulnerabilities being reported and consequently mitigated or remedied. This shows that cooperation actually works and can be extremely helpful in improving the security of information systems on which our economies and societies are so dependent. This Manifesto underlines this conclusion and is meant to show that organizations are committed to reaping the benefits of such cooperation with the cyber security community.

- The signatories of this Manifesto are committed to:
- acknowledge the efforts of (academic) researchers, penetration testers, passersby, observant users and customers, employees, well-intended hackers and everyone else to make the internet and our society more secure;
 - combine the efforts of their organization and the cyber security community in realizing a safe and secure digital society;
 - strive to remediate vulnerabilities in a correct and timely fashion;
 - combine efforts to follow international standards and best practices for remediating and disclosing vulnerabilities and implementing these in their organization. A non-comprehensive list with information on such standards and best practices can be found in Appendix A;
 - be transparent in providing information about the remediation and disclosure process;
 - join efforts to stimulate the development of international standards and best practices for remediating and disclosing vulnerabilities;
 - stimulate the international dialogue to promote the use of those mentioned mechanisms of cooperation for remedying and disclosing vulnerabilities; and
 - actively advocate the contents of this manifesto to peers.

- Taking in account that the finder of the vulnerability:
- will agree on terms and conditions for disclosure of vulnerabilities found;
 - acts in good faith; and
 - will not act disproportionately (i.e. cause unnecessary damage) when trying to find and disclose vulnerabilities.

The Dutch Cyber Security Center (NCSC) strongly encourages this private initiative.
Coordinated Vulnerability Disclosure Manifesto - April 2016

Disclosure



Disclosure Manifesto at the 2th 2016 in Amsterdam



Coordinated Vulnerability Disclosure Manifesto

Over the last decades, the importance of ICT and the role it plays in our everyday life has increased exponentially. As our interconnectedness grows and the dependence of societies on the Internet and ICT increases, the potential negative impact of vulnerabilities on ICT also increases. Consequently, finding and remedying those vulnerabilities is increasingly important.

Cooperation between organizations and the cyber security community can be used to find and fix vulnerabilities. A mechanism of cooperation that is already used in the form of *coordinated vulnerability disclosure* or *responsible disclosure*. Essentially, this is a form of cooperation in which vulnerabilities are reported to the owner of the information system, allowing the organization the opportunity to diagnose and remedy the vulnerability before the information is disclosed to third parties or the public. Further details of the coordinated vulnerability disclosure mechanism will be coordinated between the finder and the organization.

With this manifesto, initiated by Rabobank and CIO-Platform Nederland, the signatories aim to raise awareness for the importance of cooperation between organizations and the cyber security community to find and solve ICT-vulnerabilities. In the experience of the initiators, cooperation results in many vulnerabilities being reported and consequently mitigated. This shows that cooperation actually works and can be extremely helpful in improving the security of information systems on which our economies and societies are dependent. This Manifesto underlines this conclusion and is meant to show that the signatories are committed to reaping the benefits of such cooperation with the cyber security community.

- The signatories of this Manifesto are committed to:
- acknowledge the efforts of (academic) researchers, penetration testers, past and present observant users and customers, employees, well-intended hackers and even well-meaning security researchers to make the internet and our society more secure;
 - combine the efforts of their organization and the cyber security community to create a safe and secure digital society;
 - strive to remediate vulnerabilities in a correct and timely fashion;
 - combine efforts to follow international standards and best practices for remediation and disclosing vulnerabilities and implementing these in their organization. A non-comprehensive list with information on such standards and best practices can be found in Appendix A;
 - be transparent in providing information about the remediation and disclosing vulnerabilities;
 - join efforts to stimulate the development of international standards and best practices for remediation and disclosing vulnerabilities;
 - stimulate the international dialogue to promote the use of those mentioned standards and best practices for remediation and disclosing vulnerabilities; and
 - actively advocate the contents of this manifesto to peers.

Taking in account that the finder of the vulnerability:

- will agree on terms and conditions for disclosure of vulnerabilities found;
- acts in good faith; and
- will not act disproportionately (i.e. cause unnecessary damage) when trying to disclose vulnerabilities.

The Dutch Cyber Security Center (NCSC) strongly encourages this private initiative. Coordinated Vulnerability Disclosure Manifesto - April 2016



Good Practice Guide on Vulnerability Disclosure

From challenges to recommendations

NOVEMBER 2015

www.enisa.europa.eu

European Union Agency For Network And Information Security



Questions?



There are some viruses doctors can't treat.



Security



Fast response



Control



Minimized risk

