THE AVALANCHE OF VULNERABILITIES

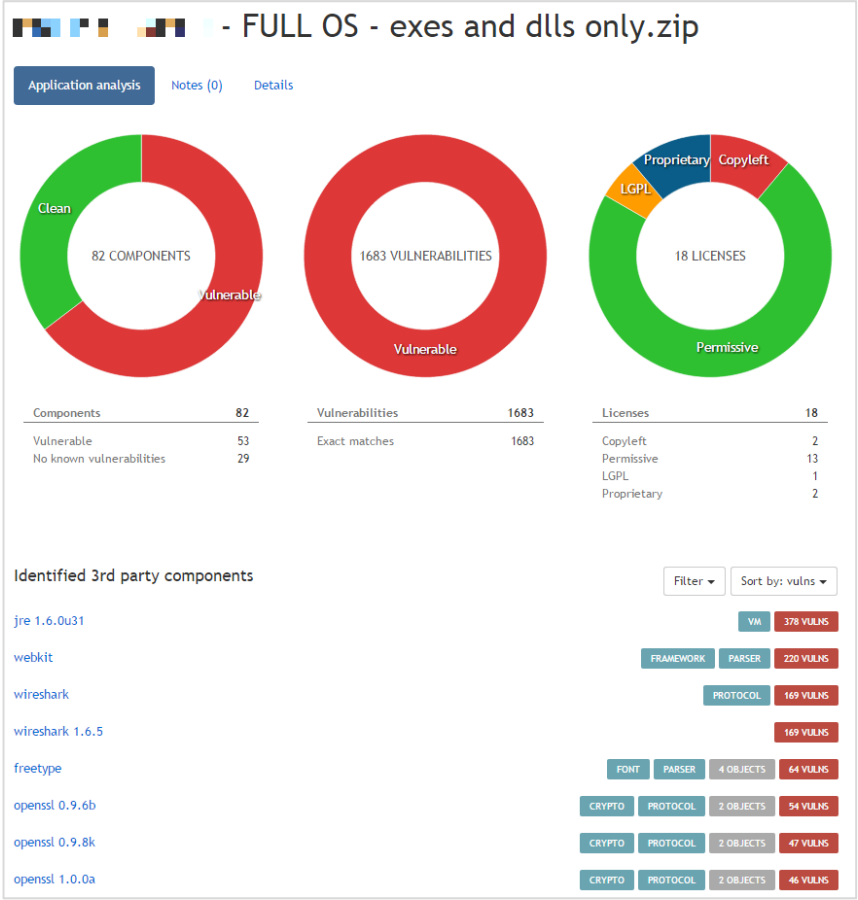
A PERSPECTIVE

Mike Ahmadi
Global Director of Critical Systems Security, Codenomicon Ltd


@codenomicon

UNKNOWN VULNERABILITIES ARE **BAD**… KNOWN VULNERABILITIES ARE A **HUGE** PROBLEM

- Hospital central monitoring system with **1683 known vulnerabilities**
- 378 of the vulnerabilities are in one (Java) runtime environment, meaning **just updating the version will fix 378 vulnerabilities.**
- This **system** is **widely used** throughout hospitals…including government hospitals



MEDICAL ISSUES ARE WIDESPREAD

Infusion Pump	Patient Monitor	Brain Wave Monitoring Device (OS)	Drug Library
			

Infusion Pump:
55 Known Vulnerabilities

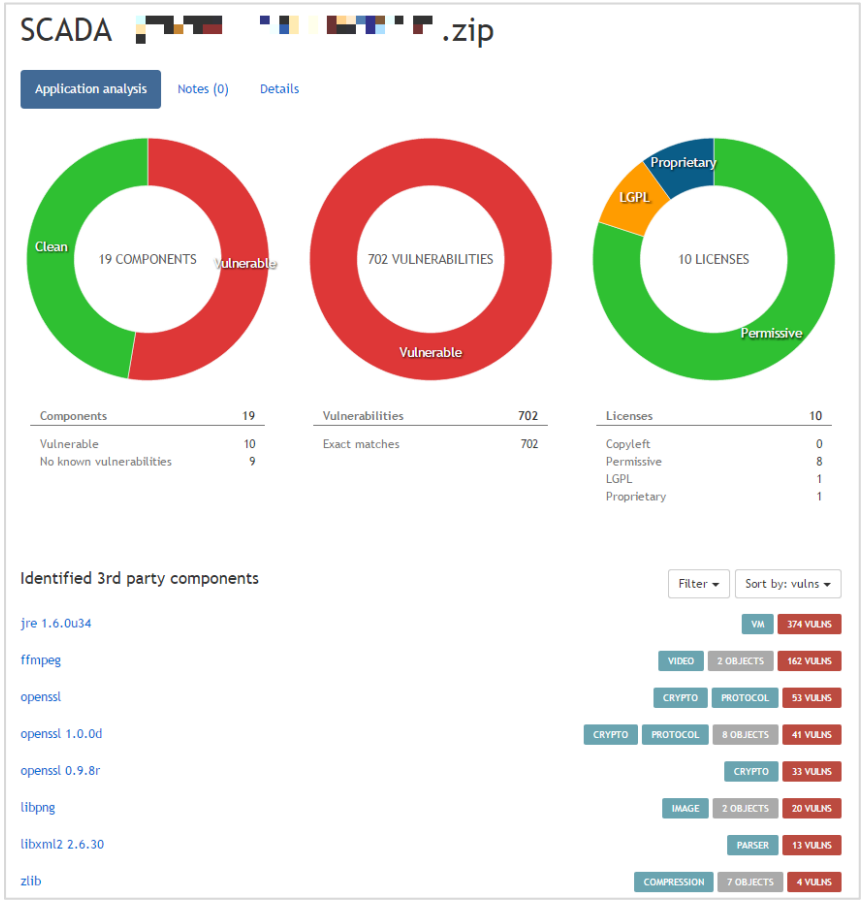
Patient Monitor:
818 Known Vulnerabilities

Brain Wave Monitoring Device:
181 Known Vulnerabilities
182 Missing Exploit Mitigation Techniques

Drug Library:
440 Known Vulnerabilities
49 Missing Exploit Mitigation Techniques

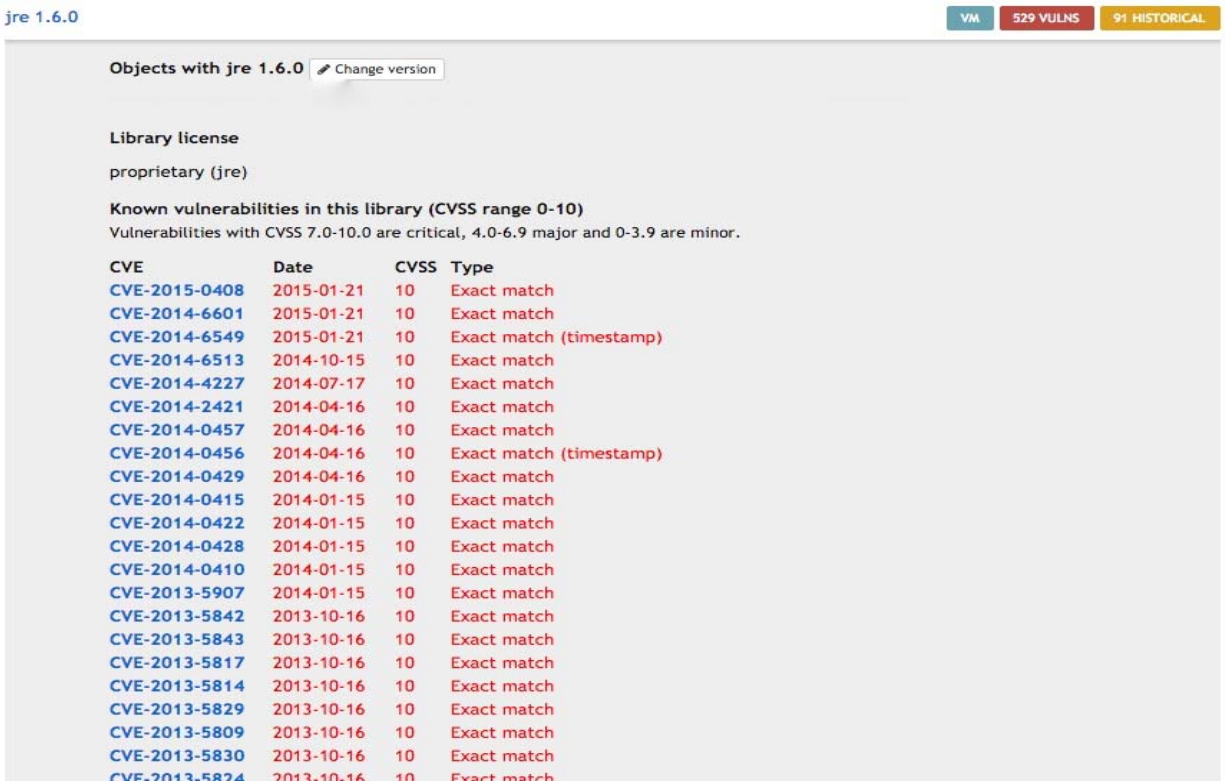
LET'S LOOK AT AN INDUSTRIAL CONTROL SYSTEM

- SCADA system with over **20,000 licenses worldwide**
- **Customer reference list on website (including government customers)**
- **702 exact match vulnerabilities** in 10 components.
- **374 vulnerabilities in 1 java runtime**
- **Over 150** NIST CVSS **critical in one component**



SERIOUS NATURE OF SPECIFIC VULNERABILITIES

- Over **150 vulnerabilities** in Java scored **CRITICAL**
- Critical commonly means **remotely executable with no authentication**
- This means that there are potentially at least **150 fairly trivial ways to exploit** the system



jre 1.6.0

VM | 529 VULNS | 91 HISTORICAL

Objects with jre 1.6.0 Change version

Library license

proprietary (jre)

Known vulnerabilities in this library (CVSS range 0-10)

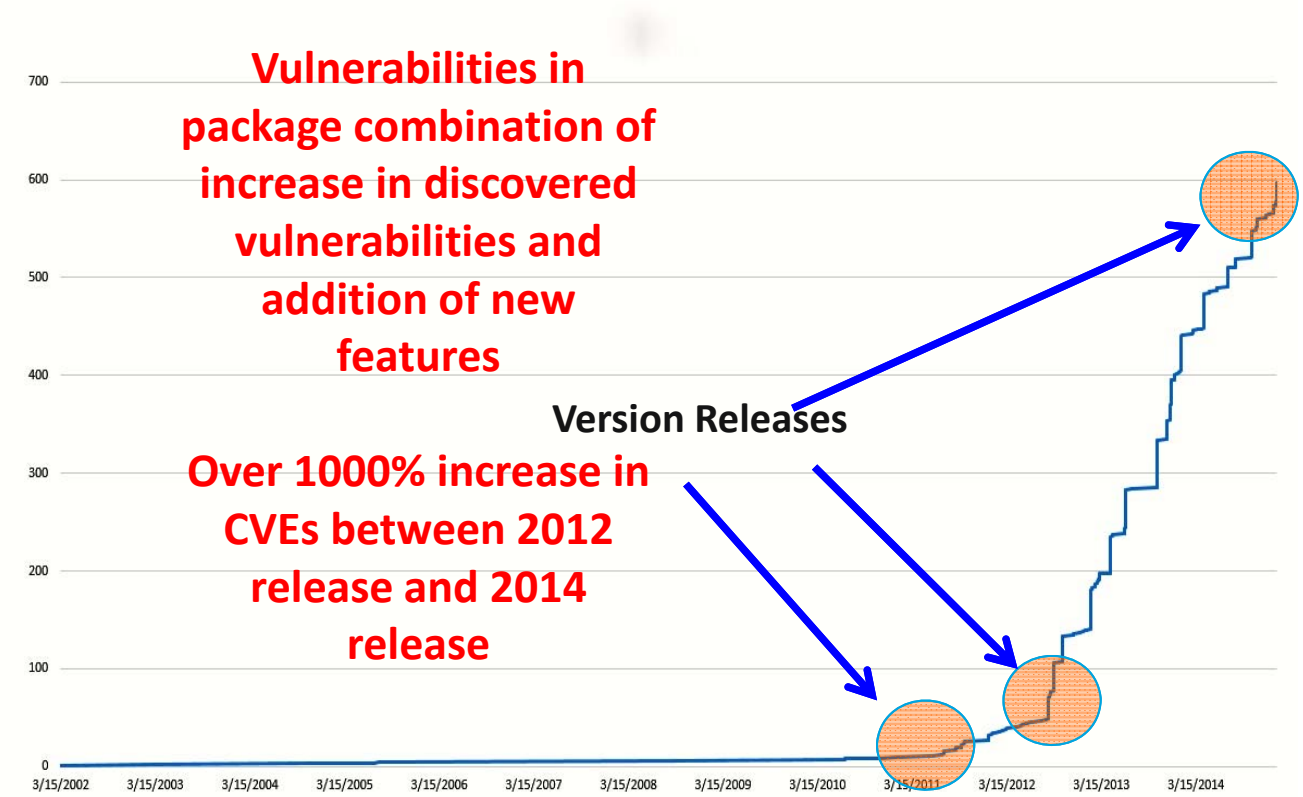
Vulnerabilities with CVSS 7.0-10.0 are critical, 4.0-6.9 major and 0-3.9 are minor.

CVE	Date	CVSS	Type
CVE-2015-0408	2015-01-21	10	Exact match
CVE-2014-6601	2015-01-21	10	Exact match
CVE-2014-6549	2015-01-21	10	Exact match (timestamp)
CVE-2014-6513	2014-10-15	10	Exact match
CVE-2014-4227	2014-07-17	10	Exact match
CVE-2014-2421	2014-04-16	10	Exact match
CVE-2014-0457	2014-04-16	10	Exact match
CVE-2014-0456	2014-04-16	10	Exact match (timestamp)
CVE-2014-0429	2014-04-16	10	Exact match
CVE-2014-0415	2014-01-15	10	Exact match
CVE-2014-0422	2014-01-15	10	Exact match
CVE-2014-0428	2014-01-15	10	Exact match
CVE-2014-0410	2014-01-15	10	Exact match
CVE-2013-5907	2014-01-15	10	Exact match
CVE-2013-5842	2013-10-16	10	Exact match
CVE-2013-5843	2013-10-16	10	Exact match
CVE-2013-5817	2013-10-16	10	Exact match
CVE-2013-5814	2013-10-16	10	Exact match
CVE-2013-5829	2013-10-16	10	Exact match
CVE-2013-5809	2013-10-16	10	Exact match
CVE-2013-5830	2013-10-16	10	Exact match
CVE-2013-5824	2013-10-16	10	Exact match

codenomicon

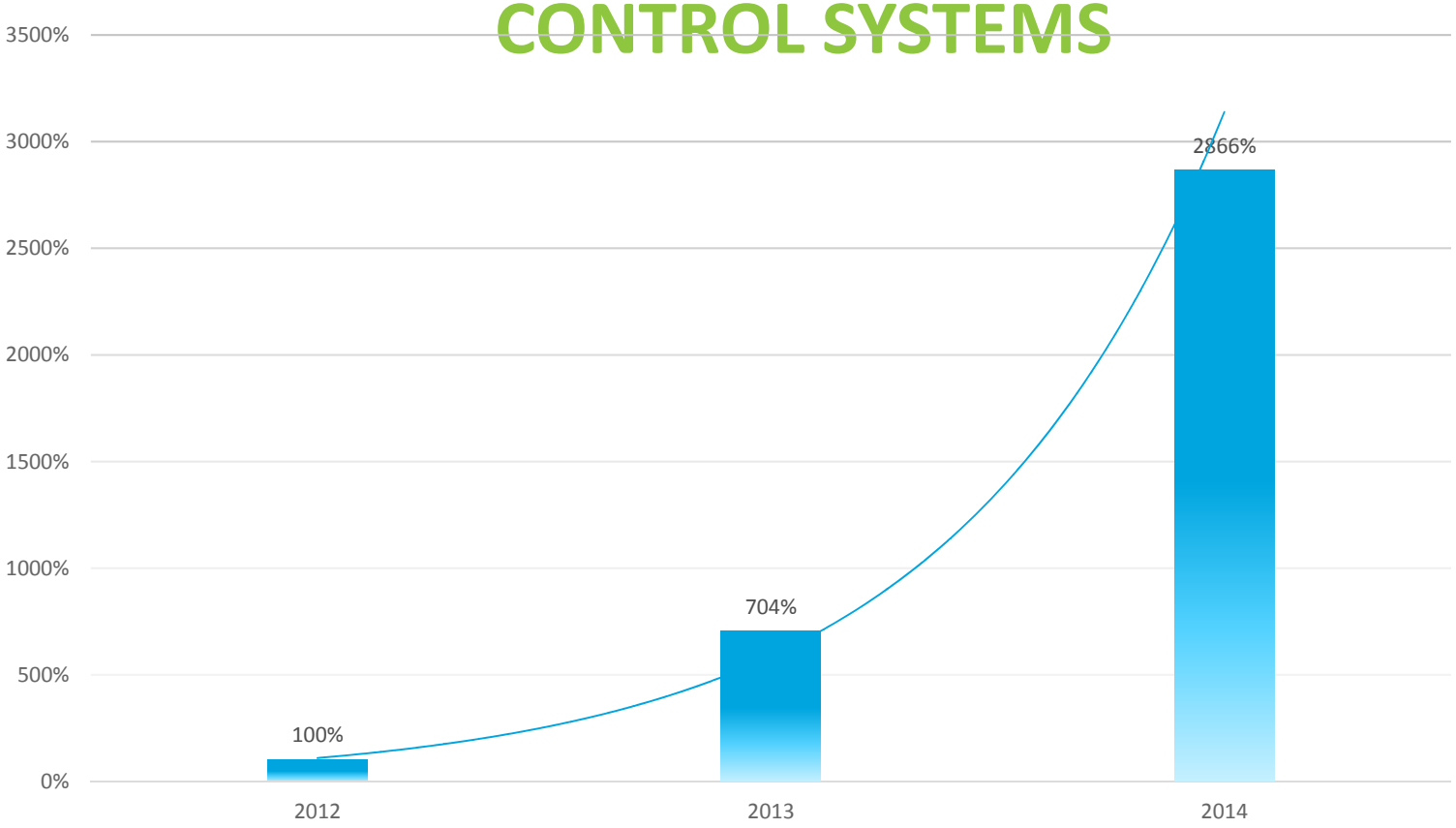
UNIQUE VULNERABILITIES GRAPH OVER TIME

- **Huge increase** in number of vulnerabilities entering **NIST CVE database** in the last 3 years
- **Massive spike since 2013** for common software components (such as Java, OpenSSL)



codenomicon

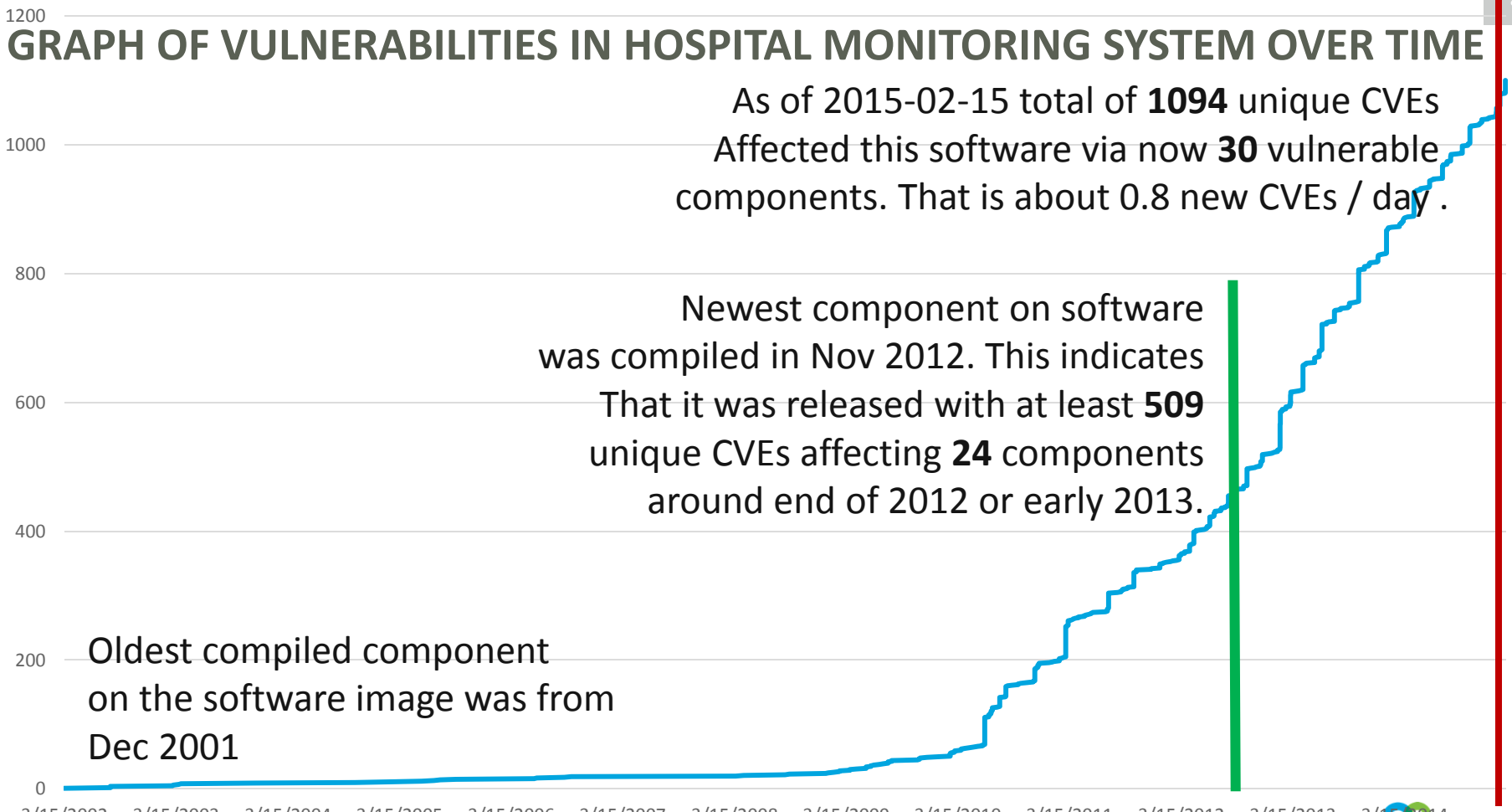
INCREASE IN MALWARE ATTACKS ON INDUSTRIAL CONTROL SYSTEMS



source: Kaspersky Labs

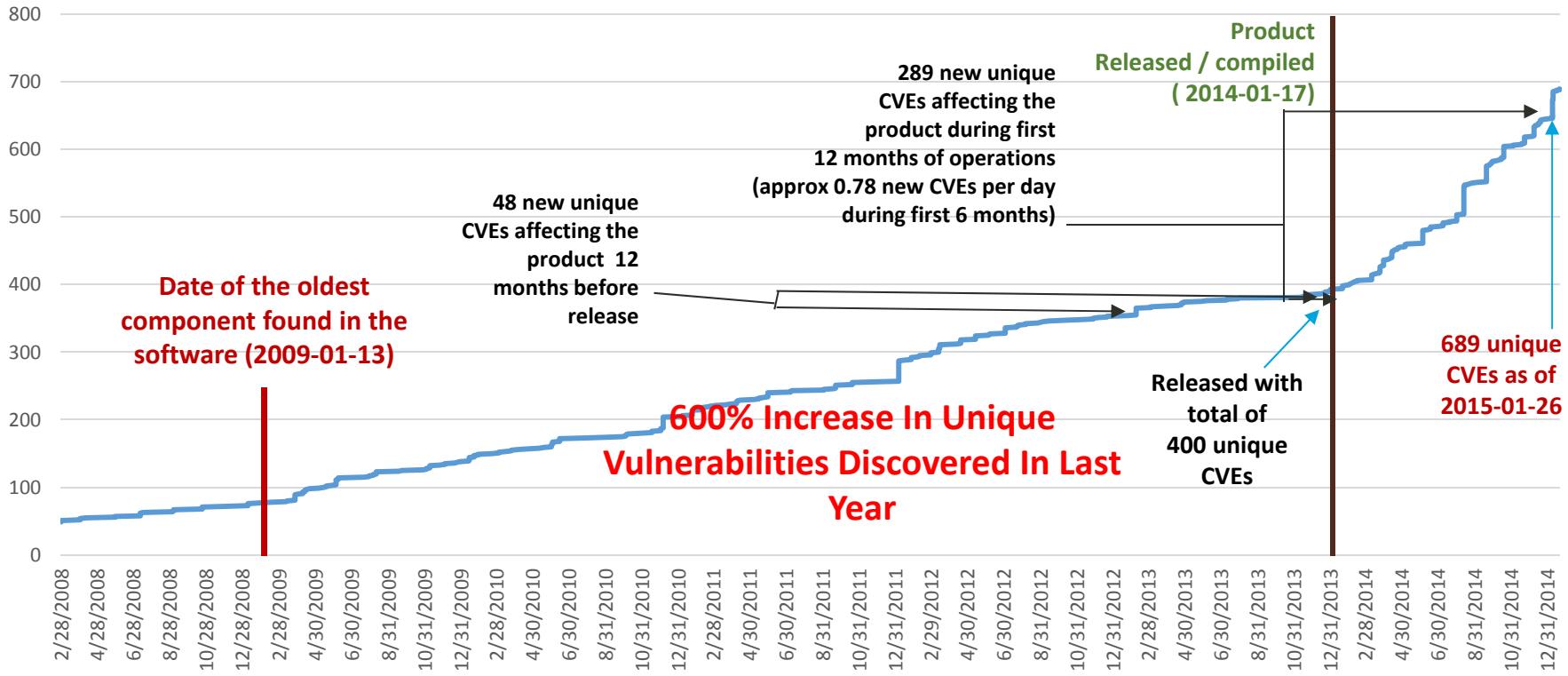
codenomicon

GRAPH OF VULNERABILITIES IN HOSPITAL MONITORING SYSTEM OVER TIME



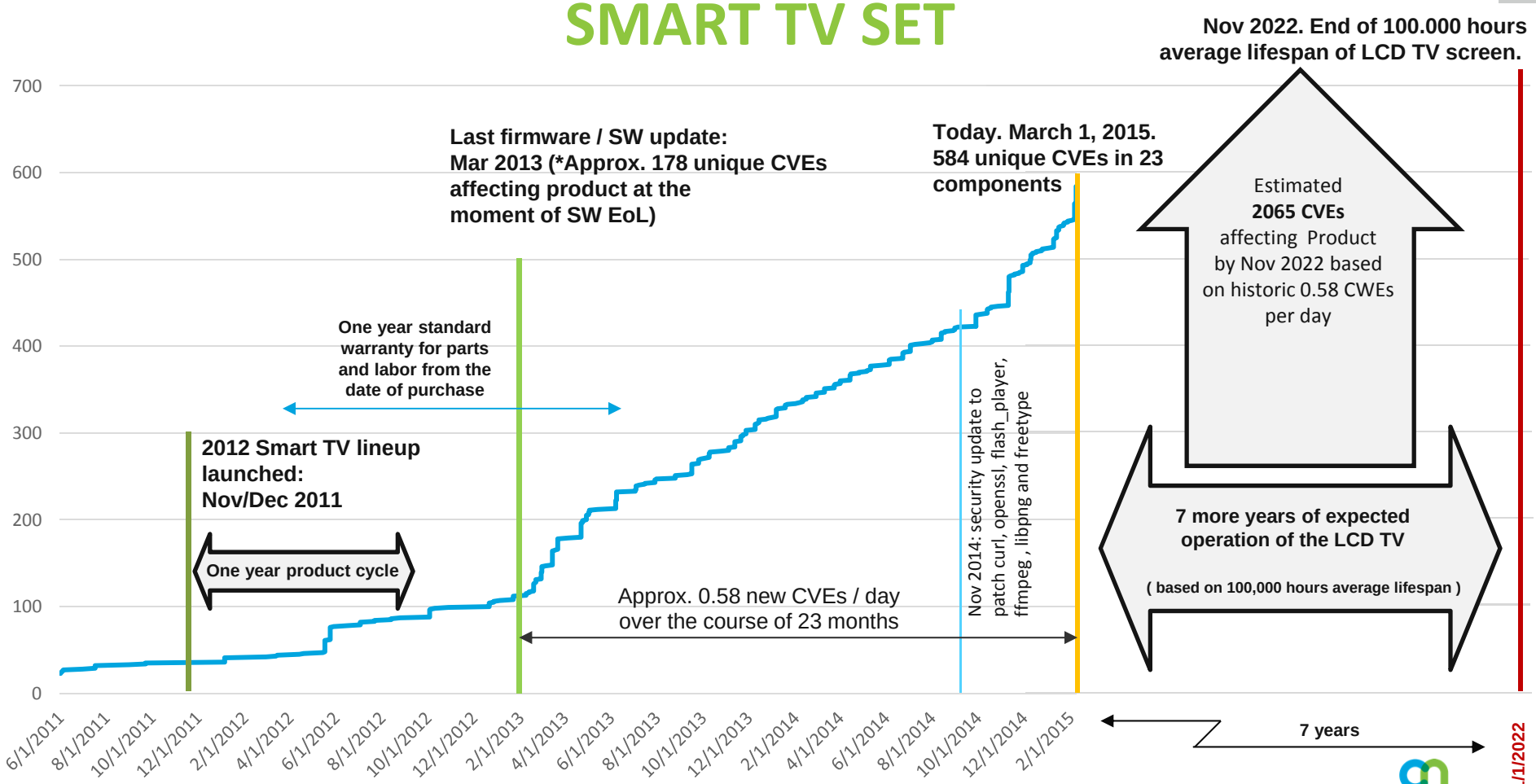
codenomicon

CODE DECAY OVER TIME – ROUTER



codenomicon

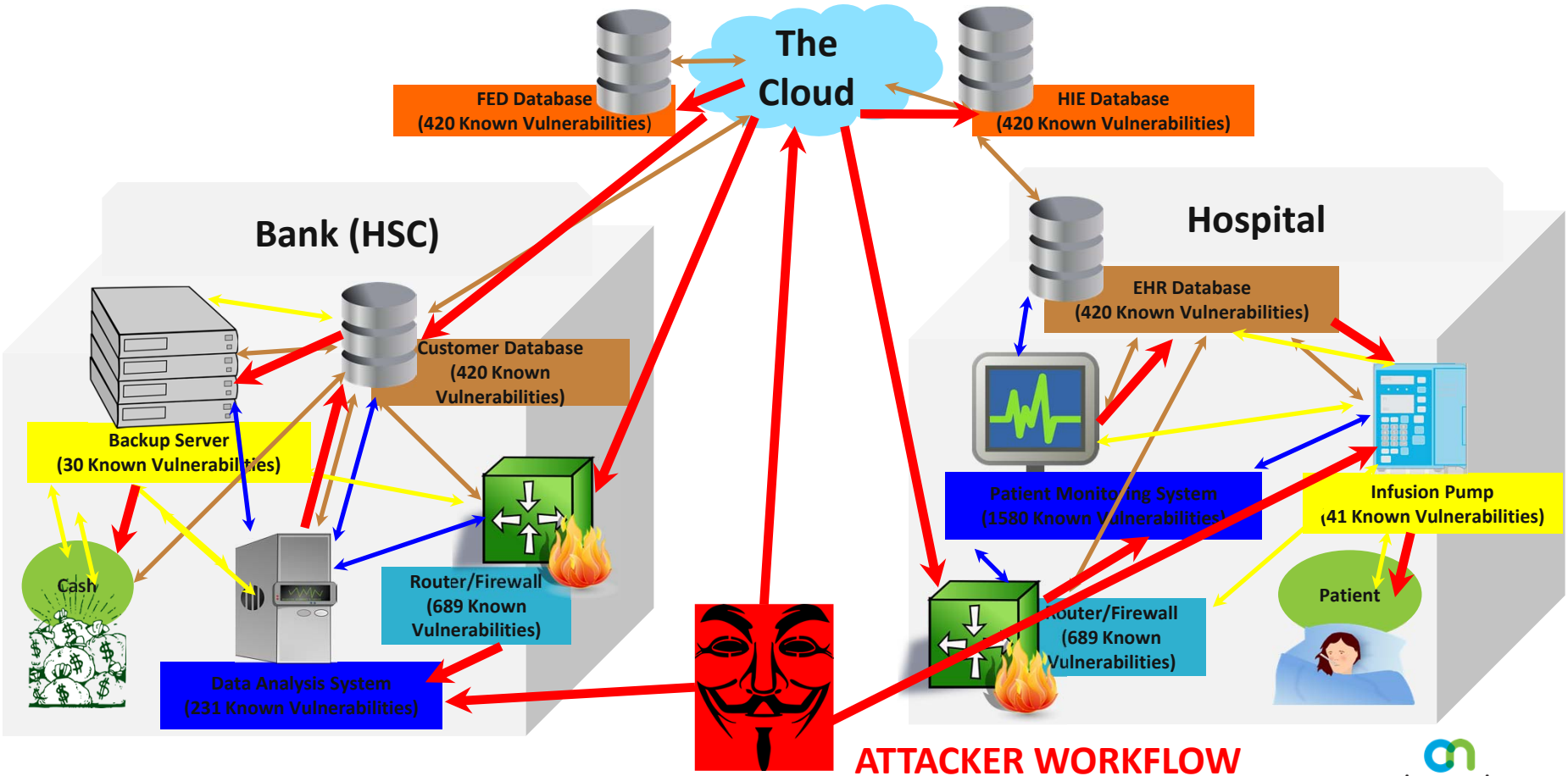
SMART TV SET



(* date may not be fully accurate, as e.g. partial OTA updates may have been delivered after this date as well (see sec. update on Nov 2014)

codenomicon

INFORMATION WORKFLOW



codenomicon

MEDJACK – NOW THERE'S A NAME FOR IT

- Report issued by security organization TrapX.
- From the article "TrapX found that while many hospitals, for example, maintain solid IT departments with firewalls and other security solutions, these vulnerable medical devices are often left without patching."
- Attacker uses unpatched devices to get wherever they want to go.

Source:http://www.scmagazine.com/trapx-profiles-medjack-threat/article/418811/

June 04, 2015

'MEDJACK' tactic allows cyber criminals to enter healthcare networks undetected

Share this article:

This year has already been marked by data breaches at multiple major healthcare organizations, including CareFirst BlueCross BlueShield and Anthem. While these providers have pointed to various causes and attacks as the source of their compromises, not yet has it become prominent news that medical organizations' devices might be the true culprit behind many already and soon-to-be-discovered breaches.

TrapX published a report on "medical device hijack," or MEDJACK, which allows attackers to build backdoors into healthcare providers' networks.

A report from TrapX found that a majority of organizations are vulnerable, if not already victim to MEDJACK, or "medical device hijack." Essentially, the company wrote, attackers maneuver though healthcare systems' main networks by initially exploiting outdated and unpatched medical devices, such as an X-ray scanner or blood gas analyzer. They build backdoors into the systems through these internet-connected devices.

"Our scientists have observed that you could manufacture an attack, designed specifically for several models of a specific medical device, and then launch that attack," wrote Carl Wright, general manager at TrapX in an email to SCMagazine.com. "That, combined with the difficulty in diagnosis and remediation, and the very high value of healthcare data, create a near perfect target for organized crime."

Through various case studies, TrapX found that while many hospitals, for example, maintain solid IT departments with firewalls and other security solutions, these vulnerable medical devices are often left without patching. Generally, the security team is unable to fully view the device console or operating system, and because these machines often run for days, there's never a time to disconnect them entirely.

codenomicon

ROYCE BILL: CYBER SUPPLY CHAIN MANAGEMENT AND TRANSPARENCY ACT – KEY PROVISIONS

- For government agencies, software contracts must include clauses requiring:
  - a confidentially supplied list, or a bill of materials, of each binary component that is used in the software, firmware, or product;
  - the contractor to verify that products do not contain known security vulnerabilities and to notify the purchasing agency of any known vulnerabilities or defects;
  - product designs to allow fixes with patches, updates, or replacements; and
  - the contractor to provide timely repairs for discovered vulnerabilities.

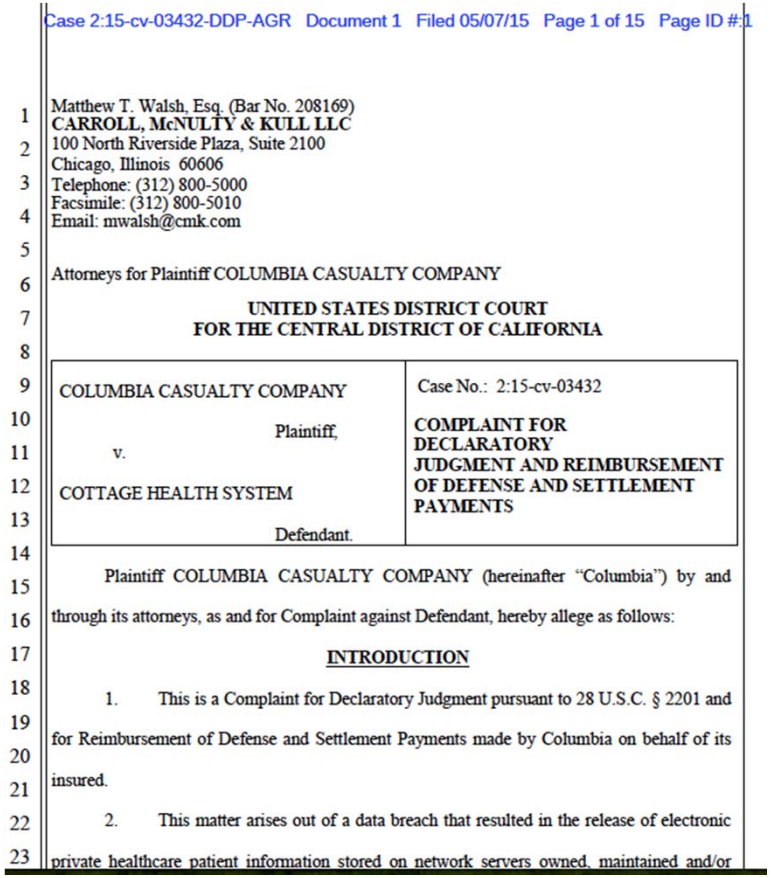
OPPOSITION ARGUMENTS

- **We already do this:** The data indicates that if this is already being done no action is being taken to resolve the issue. More likely it is not being done…or being done quite poorly, and leaving us all at risk.
- **Sharing a Bill of Materials means giving up proprietary information:** FDA already requires an ingredient list. Coca Cola can supply an ingredient list without sharing trade secrets.
- **I cannot control my supply chain:** You already do in selection of products based on feature requirements.
- **This requires too much work:** Tools are completely automated and easy to use.
- **This bill is being backed by organizations that stand to benefit from such legislation:** Actually, we all benefit from better security. The entire software security industry is built on identifying and mitigating security issues.

codenomicon

THE INSURANCE INDUSTRY PUSHES BACK

- Cottage Health System gets breached forced to pay class action settlement of $4.125 million ($81 per record)
- Insurer files suit in court for a Declaratory Judgment against Columbia for Cottage's "**Failure to Follow Minimum Required Practices.**"



Case 2:15-cv-03432-DDP-AGR Document 1 Filed 05/07/15 Page 1 of 15 Page ID #:1

Matthew T. Walsh, Esq. (Bar No. 208169)
CARROLL, McNULTY & KULL LLC
100 North Riverside Plaza, Suite 2100
Chicago, Illinois 60606
Telephone: (312) 800-5000
Facsimile: (312) 800-5010
Email: mwalsh@cmk.com

Attorneys for Plaintiff COLUMBIA CASUALTY COMPANY

UNITED STATES DISTRICT COURT
FOR THE CENTRAL DISTRICT OF CALIFORNIA

COLUMBIA CASUALTY COMPANY Plaintiff, v. COTTAGE HEALTH SYSTEM Defendant.	Case No.: 2:15-cv-03432 **COMPLAINT FOR DECLARATORY JUDGMENT AND REIMBURSEMENT OF DEFENSE AND SETTLEMENT PAYMENTS**

Plaintiff COLUMBIA CASUALTY COMPANY (hereinafter "Columbia") by and through its attorneys, as and for Complaint against Defendant, hereby allege as follows:

INTRODUCTION

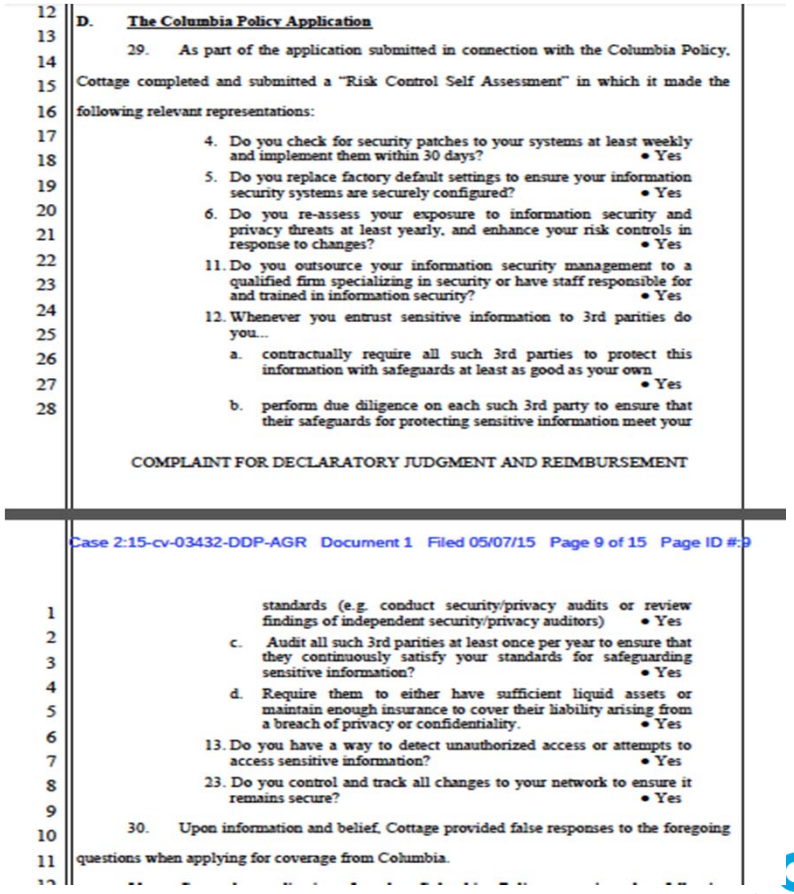
1. This is a Complaint for Declaratory Judgment pursuant to 28 U.S.C. § 2201 and for Reimbursement of Defense and Settlement Payments made by Columbia on behalf of its insured.

2. This matter arises out of a data breach that resulted in the release of electronic private healthcare patient information stored on network servers owned, maintained and/or

codenomicon

SOME MINIMUM REQUIRED PRACTICES IN DETAIL

- Check for security patches and apply within 30 days
- Replace factory default settings
- Re-assess risk yearly and apply changes
- Require 3rd parties to protect information with safeguards at least as good as your own
- **PERFORM DUE DILLIGENCE ON 3RD PARTIES TO ENSURE THAT THEIR SAFEGUARDS ARE AS GOOD AS YOUR OWN**
- **AUDIT 3RD PARTIES TO ENSURE THEY CONTINUOSLY SATISFY YOUR STANDARDS FOR SAFEGUARDING SENSITIVE INFORMATION**



D. **The Columbia Policy Application**

29. As part of the application submitted in connection with the Columbia Policy, Cottage completed and submitted a "Risk Control Self Assessment" in which it made the following relevant representations:

4. Do you check for security patches to your systems at least weekly and implement them within 30 days? • Yes
5. Do you replace factory default settings to ensure your information security systems are securely configured? • Yes
6. Do you re-assess your exposure to information security and privacy threats at least yearly, and enhance your risk controls in response to changes? • Yes
11. Do you outsource your information security management to a qualified firm specializing in security or have staff responsible for and trained in information security? • Yes
12. Whenever you entrust sensitive information to 3rd parities do you...
    a. contractually require all such 3rd parties to protect this information with safeguards at least as good as your own • Yes
    b. perform due diligence on each such 3rd party to ensure that their safeguards for protecting sensitive information meet your

COMPLAINT FOR DECLARATORY JUDGMENT AND REIMBURSEMENT

Case 2:15-cv-03432-DDP-AGR Document 1 Filed 05/07/15 Page 9 of 15 Page ID #:9

standards (e.g. conduct security/privacy audits or review findings of independent security/privacy auditors) • Yes
    c. Audit all such 3rd parities at least once per year to ensure that they continuously satisfy your standards for safeguarding sensitive information? • Yes
    d. Require them to either have sufficient liquid assets or maintain enough insurance to cover their liability arising from a breach of privacy or confidentiality. • Yes
13. Do you have a way to detect unauthorized access or attempts to access sensitive information? • Yes
23. Do you control and track all changes to your network to ensure it remains secure? • Yes

30. Upon information and belief, Cottage provided false responses to the foregoing questions when applying for coverage from Columbia.

codenomicon

BUILDING A CYBERSECURITY CERTIFICATION LAB

Company Offerings Standards Dashboard

NEWSROOM / Press Releases

UL LLC Collaborates with Codenomicon to Test Industrial Automation Equipment and Services and Medical Devices for Digital Security Vulnerabilities

NORTHBROOK, Ill., April 13, 2015 — UL and Codenomicon have collaborated to develop and perform security testing on network connected devices. Initial testing will be on industrial automation equipment and services and medical devices, with planned expansion into security testing in other industries. Codenomicon and UL will work together to provide Fuzz and Binary Analysis testing services. Fuzz Testing is a mechanism in which the communication protocols of the device under test are subjected to random exception messages to discover coding and security errors. The Binary Analysis identifies known vulnerabilities found in compiled software that could possibly be deployed in a production environment.

- **Aligned with international standards (62443)**
- **Creating program due to demand**
- **Creating program due to need**
- **Active lobbying to promote message**

codenomicon

Mike Ahmadi
Global Director, Critical Systems Security
Codenomicon Ltd.

Phone: (925) 413-4365
Email: Mike@Codenomicon.com

codenomicon

questions


codenomicon