Weaving a Fabric of Trust

Ensured Security, Privacy, Resilience, and Accountability

Dr. Greg Shannon
Chief Scientist

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

First Bits

Congressional Testimony on Understanding the Cyber Threat and Implications for the 21st Century Economy

Mar 3, 2015 U.S. House of Representatives

(114th Congress)

Hearing before the Subcommittee on Oversight and Investigations of the Committee on Energy and Commerce.

Question was…

“How do businesses deal with consumers and inform and educate them as to what they are doing to create the virtual marketplace, and prohibit incursions in cyber?”

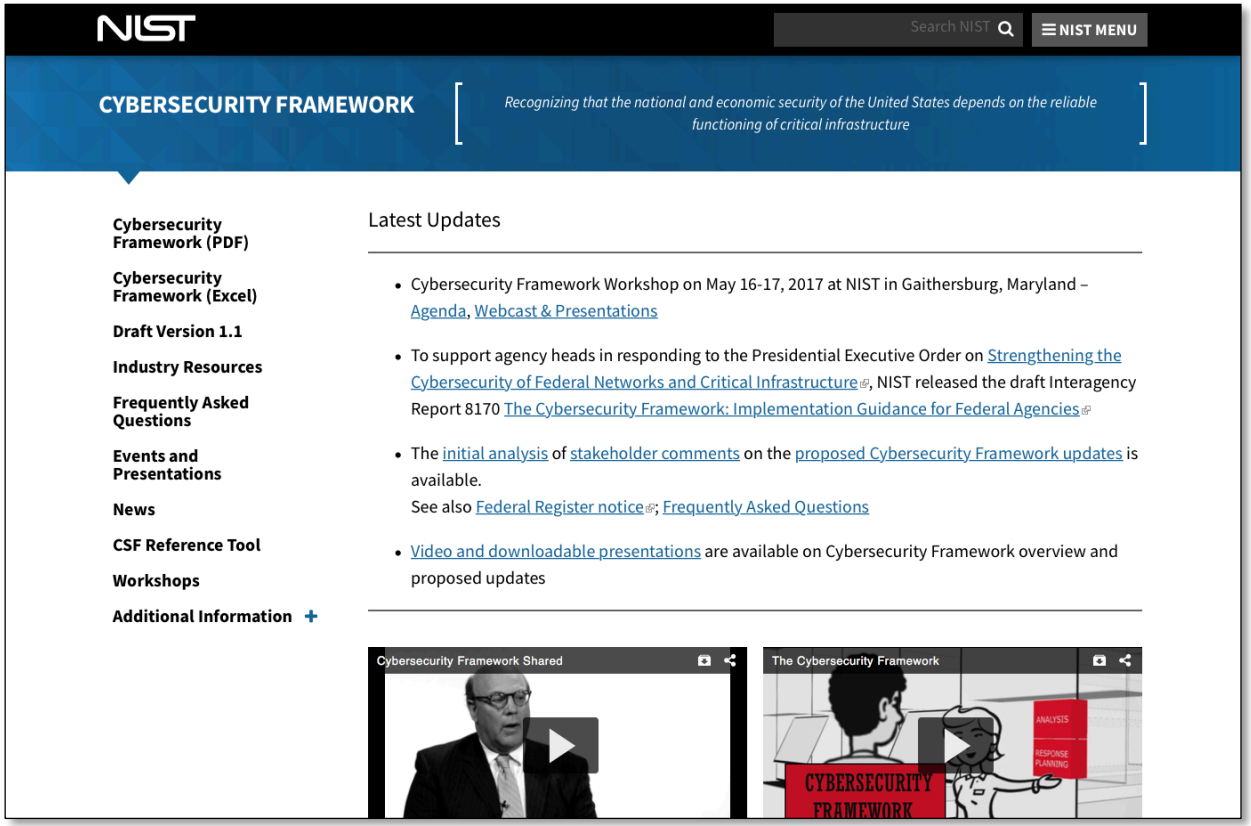
E WHITE
WASHINGT

Consistent Approach


Official White House Photo by Chuck Kennedy


Associated Press/Pablo Martinez Monsivais

NIST Framework



Building the Future

What’s the problem we’re trying to solve?

Building the Future

What’s the hard part of the problem?

Building the Future

Where’s the “promise of possibility”?

Building the Future

What can we do?

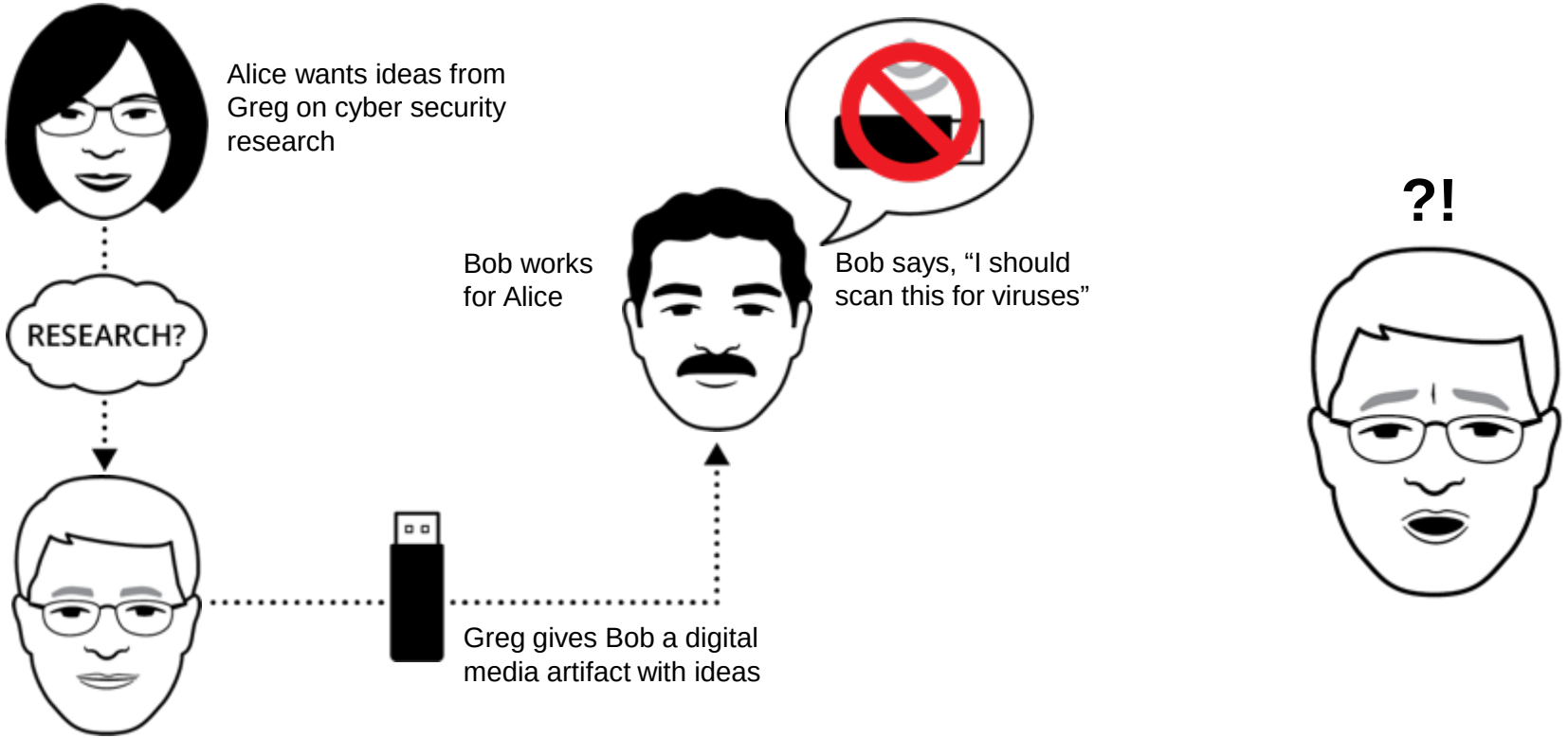
What can YOU do?!?

Let’s do it.

The Takeaway

Trust

2006 Aha! Trust Rabbit Hole



Digital Intermediation?

What might we lose?

What might we gain?

The Essence of Trust

Trust in a Digital World

Building Trust

Breaking Trust

Engineering Dilemmas

Engineering Trust

Security

Privacy

Resiliency

Accountability

Trust Poll

What matters MOST to you in building, growing, and sustaining TRUST?

* Security
* Privacy
* Resilience
* Accountability

Discussion

Ensure

Cyber Delusions

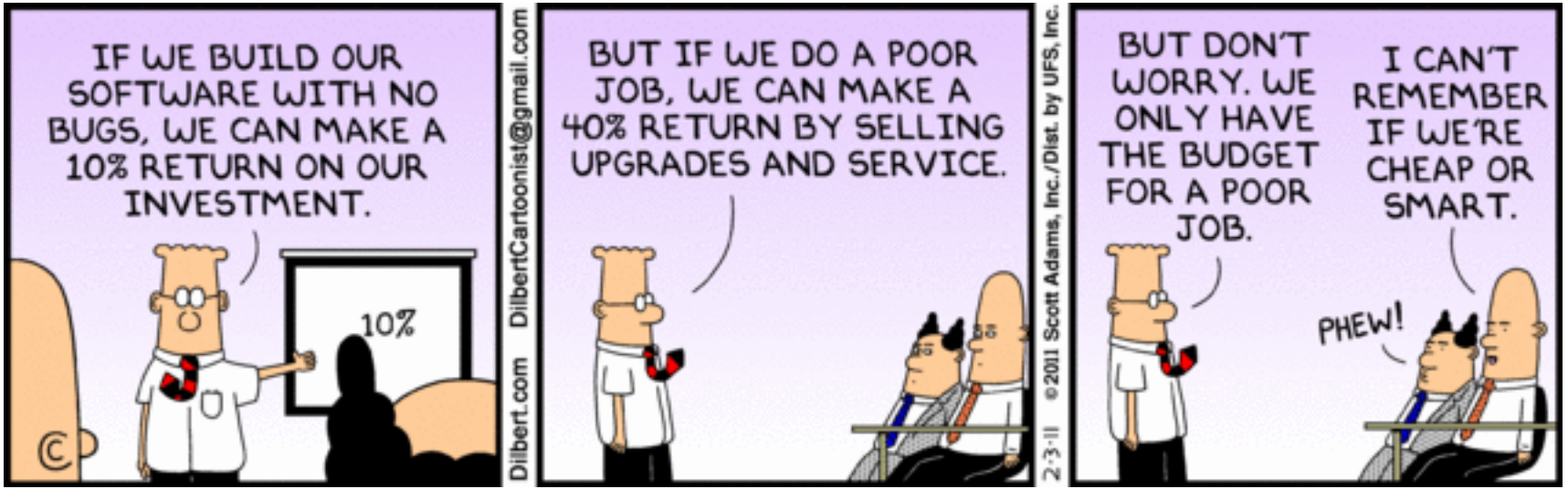
Cyber Delusions

Cyber Delusions

Cyber Delusions

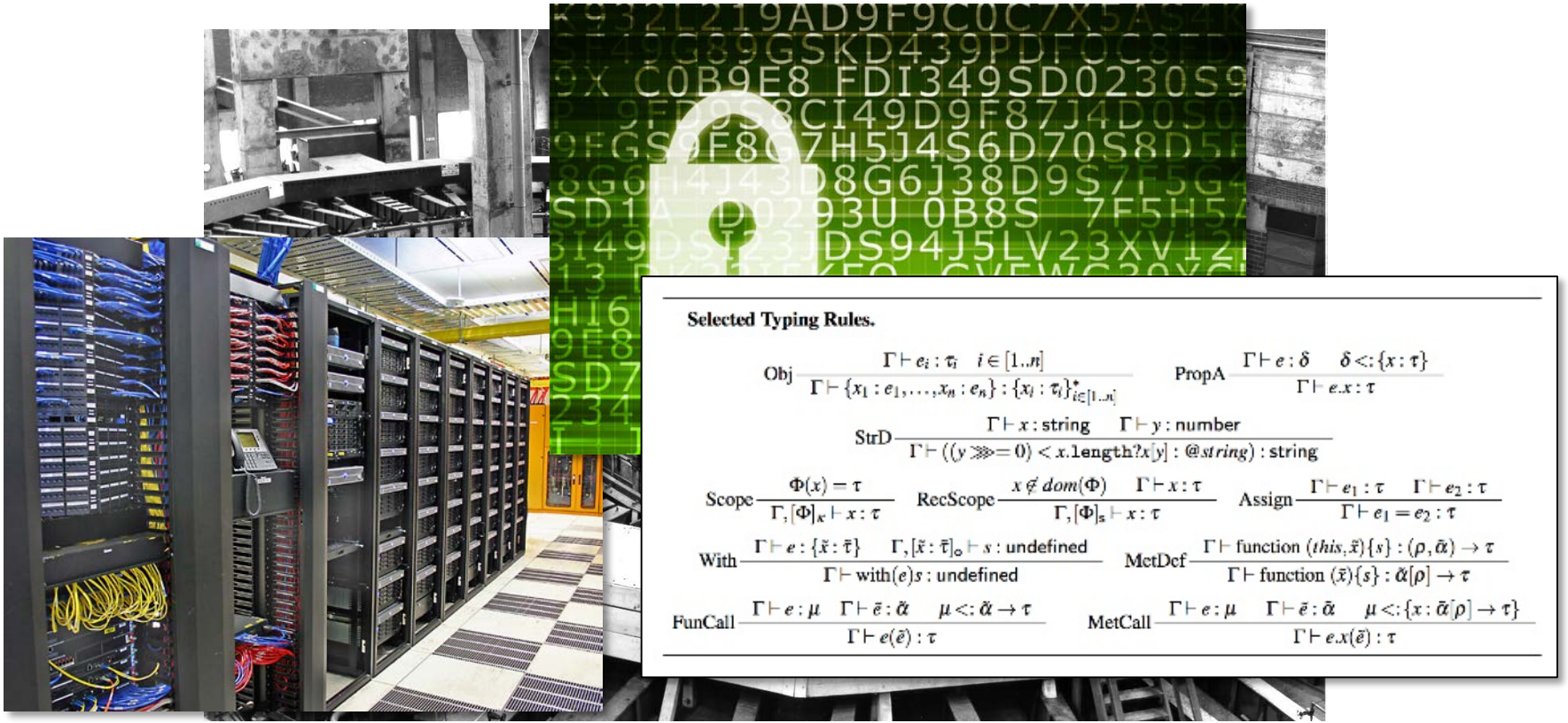
PHOTO: JOHN R. COUGHLIN/CNNMONEY

Security Built in?



http://www.dilbert.com/strips/2011-02-03/

2014 Aha! Cyber Energy Barrier



Selected Typing Rules.

$$\text{Obj}\ \frac{\Gamma \vdash e_i : \tau_i \quad i \in [1..n]}{\Gamma \vdash \{x_1 : e_1, \ldots, x_n : e_n\} : \{x_i : \tau_i\}^{*}_{i \in [1..n]}} \qquad \text{PropA}\ \frac{\Gamma \vdash e : \delta \quad \delta <: \{x : \tau\}}{\Gamma \vdash e.x : \tau}$$

$$\text{StrD}\ \frac{\Gamma \vdash x : \text{string} \quad \Gamma \vdash y : \text{number}}{\Gamma \vdash ((y \ggg= 0) < x.\texttt{length}?x[y] : @string) : \text{string}}$$

$$\text{Scope}\ \frac{\Phi(x) = \tau}{\Gamma, [\Phi]_x \vdash x : \tau} \qquad \text{RecScope}\ \frac{x \notin dom(\Phi) \quad \Gamma \vdash x : \tau}{\Gamma, [\Phi]_s \vdash x : \tau} \qquad \text{Assign}\ \frac{\Gamma \vdash e_1 : \tau \quad \Gamma \vdash e_2 : \tau}{\Gamma \vdash e_1 = e_2 : \tau}$$

$$\text{With}\ \frac{\Gamma \vdash e : \{\vec{x} : \vec{\tau}\} \quad \Gamma, [\vec{x} : \vec{\tau}]_\circ \vdash s : \text{undefined}}{\Gamma \vdash \text{with}(e)s : \text{undefined}} \qquad \text{MetDef}\ \frac{\Gamma \vdash \text{function}\ (this, \vec{x})\{s\} : (\rho, \vec{\alpha}) \to \tau}{\Gamma \vdash \text{function}\ (\vec{x})\{s\} : \vec{\alpha}[\rho] \to \tau}$$

$$\text{FunCall}\ \frac{\Gamma \vdash e : \mu \quad \Gamma \vdash \vec{e} : \vec{\alpha} \quad \mu <: \vec{\alpha} \to \tau}{\Gamma \vdash e(\vec{e}) : \tau} \qquad \text{MetCall}\ \frac{\Gamma \vdash e : \mu \quad \Gamma \vdash \vec{e} : \vec{\alpha} \quad \mu <: \{x : \vec{\alpha}[\rho] \to \tau\}}{\Gamma \vdash e.x(\vec{e}) : \tau}$$

Elements of Defensive Deterrence

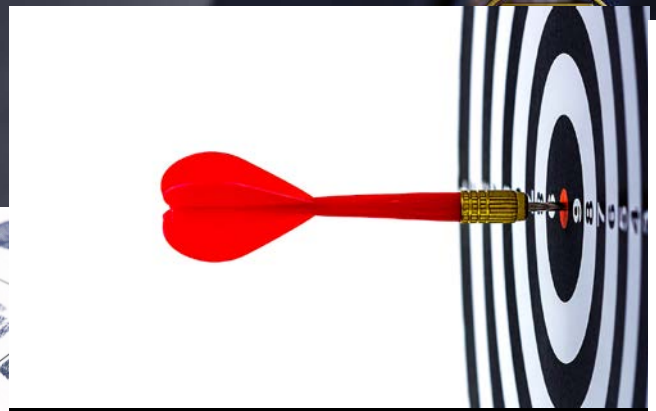
Impose extreme/intractable resource requirements on adversaries

Ensure that small breaches/successes are minor

Ensure that significant attacks are detectible and attributable and recoverable

3 E's for Cybersecurity

Evidence



Efficacy

Efficiency

Foundations for Weaving Trust

Encryption

- Secure communication in the presence of adversaries

Formal Methods

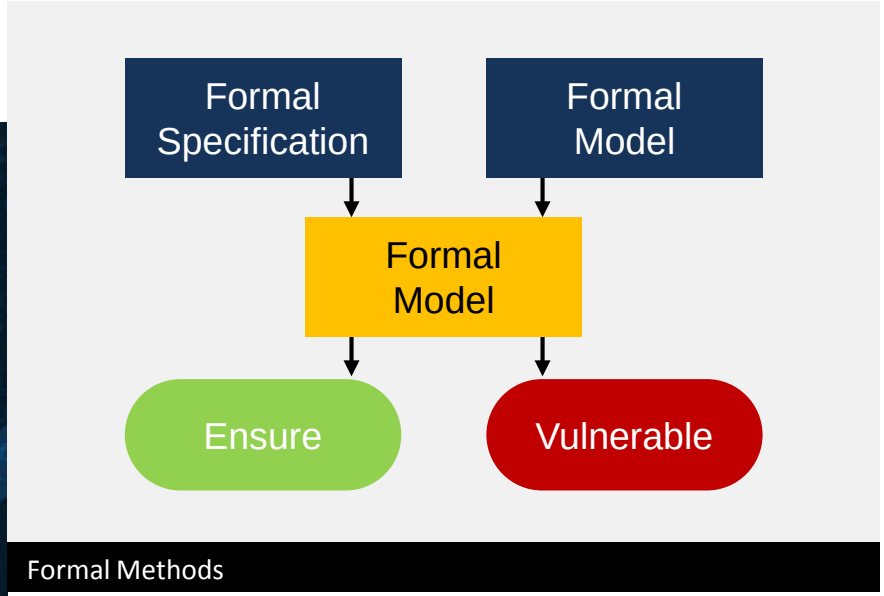
- Logic-based techniques for the specification, development, and verification of protocols, software, hardware, and systems

Long-term goal

- Weave together formal methods (warp) with encryption (weft) to expand security, privacy, resilience, accountability

Recent Advances

Encryption



Formal Methods

Ensure Poll

What matters MOST to your organization in **THWARTING** malicious cyber activity?

UNDISCOVERABLE vulnerabilities

UNEXPLOITABLE vulnerabilities

DETECT malicious activities

ATTRIBUTE malicious actors

RECOVER from malicious activities

Discussion

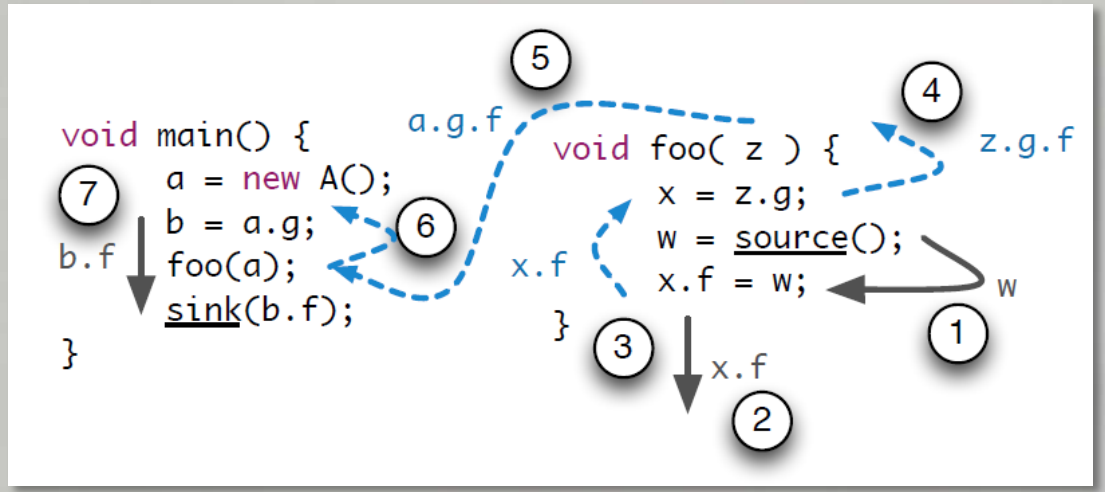
Technologies

1994 Aha! Simple Technology

Startup!

Block Bit Coin Chain

Android App Sets: Sensitive Dataflow



Cost of Failure

POLITICO

Magazine Policy PRO U.S. Edition

Facebook
Twitter
Google +
Email
Comment
Print

Acting U.S. Attorney for Vermont Eugenia Cowles announces a $155 million settlement to be paid by eClinicalWorks to resolve allegations it misrepresented the abilities of its software and paid kickbacks. | AP Photo

Feds levy $155M fine against software vendor for faulty patient records

By **ARTHUR ALLEN** | 05/31/2017 06:56 PM EDT

Share on Facebook Share on Twitter

A leading electronic health records maker and its founders will pay $155 million to resolve a lawsuit that accused the company of selling faulty software and defrauding the program that subsidized doctors to computerize their patient records, the Justice Department announced Wednesday.

The settlement, the first of its kind involving a health IT company, also states that Massachusetts-based eClinicalWorks paid kickbacks in exchange for promoting its

MOST READ

What you can do

Evidence

Efficacy

Efficiency

Technology Poll

What is YOUR outlook on cybersecurity for the next **DECADE**?

very optimistic

optimistic

neutral

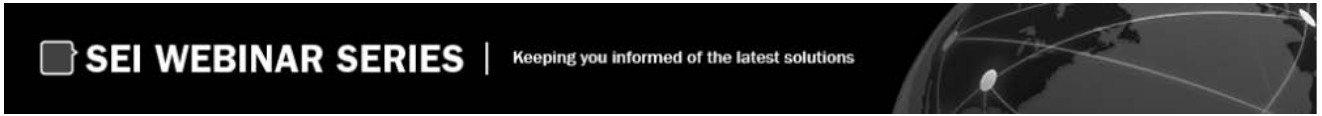
pessimistic

very pessimistic

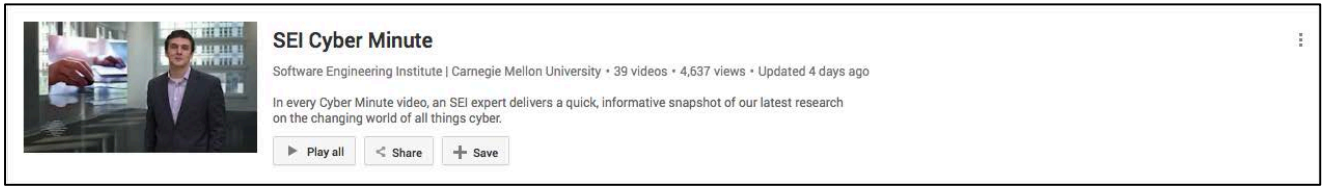
Discussion

SEI /CERT Resources

- SEI Blog(s)



- SEI Webinars



- SEI Cyber Minutes

- SEI Podcasts

Reading

David DeSteno. *The Truth about Trust.* Hudson Street Press, 2014,

Virgil Gligor and Jeannette M. Wing. 2011. Towards a theory of trust in networks of humans and computers. In *Proceedings of the 19th international conference on Security Protocols* (SP'11), Bruce Christianson, Bruno Crispo, James Malcolm, and Frank Stajano (Eds.). Springer-Verlag, Berlin, Heidelberg, 223-242. DOI=http://dx.doi.org/10.1007/978-3-642-25867-1_22

Ken Thompson. 2007. Reflections on trusting trust. In *ACM Turing award lectures*. ACM, New York, NY, USA , pages. DOI=http://dx.doi.org/10.1145/1283920.1283940

K. Fisher, J. Launchbury, and R. Richards. The HACMS Program: Using formal methods to eliminate exploitable bugs. Philosophical Transactions A. Forthcoming.

B.Fuller, et al. 2017. Cryptographically Protected Database Search (Systemization of Knowledge Paper). To appear in *Proceedings of the 2017 IEEE Symposium on Security and Privacy* (SP '17). IEEE Computer Society, Washington, DC, USA.

Contact Information

Dr. Greg Shannon

Chief Scientist

CERT Division | Software Engineering Institute

Carnegie Mellon University

Telephone: +1 412-268-8545

Email: shannon@cert.org

U.S. Mail

Software Engineering Institute

Customer Relations

4500 Fifth Avenue

Pittsburgh, PA 15213-2612

USA

Web

www.sei.cmu.edu

Customer Relations

Email: info@sei.cmu.edu

Telephone: +1 412-268-5800