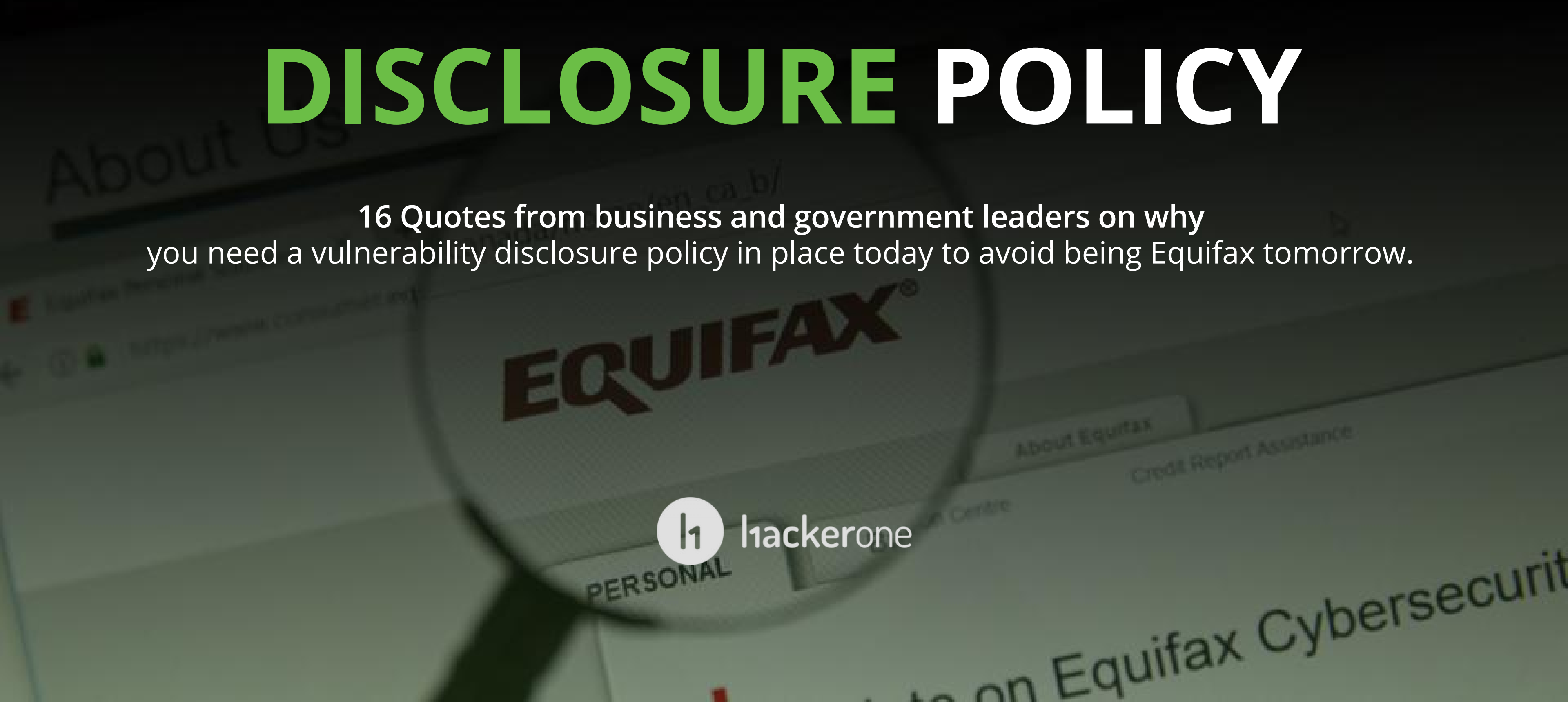
VOICES OF VULNERABILITY DISCLOSURE POLICY

16 Quotes from business and government leaders on why
you need a vulnerability disclosure policy in place today to avoid being Equifax tomorrow.



hackerone

> **All companies should consider promulgating a vulnerability disclosure policy,** that is, a public invitation for white hat security researchers to report vulnerabilities. The U.S. Department of Defense runs such a program. It has been very successful in finding and solving problems before they turn into crises.

ROD J. ROSENSTEIN
Deputy Attorney General, U.S. Department of Justice

https://www.justice.gov/opa/speech/deputy-attorney-general-rod-j-rosenstein-delivers-remarks-global-cyber-security-summit

> To improve the security of their connected systems, **every corporation should have a vulnerability disclosure policy** that allows them to receive security submissions from the outside world.

JEFF MASSIMILLA
Chief Product Cybersecurity Officer, General Motors

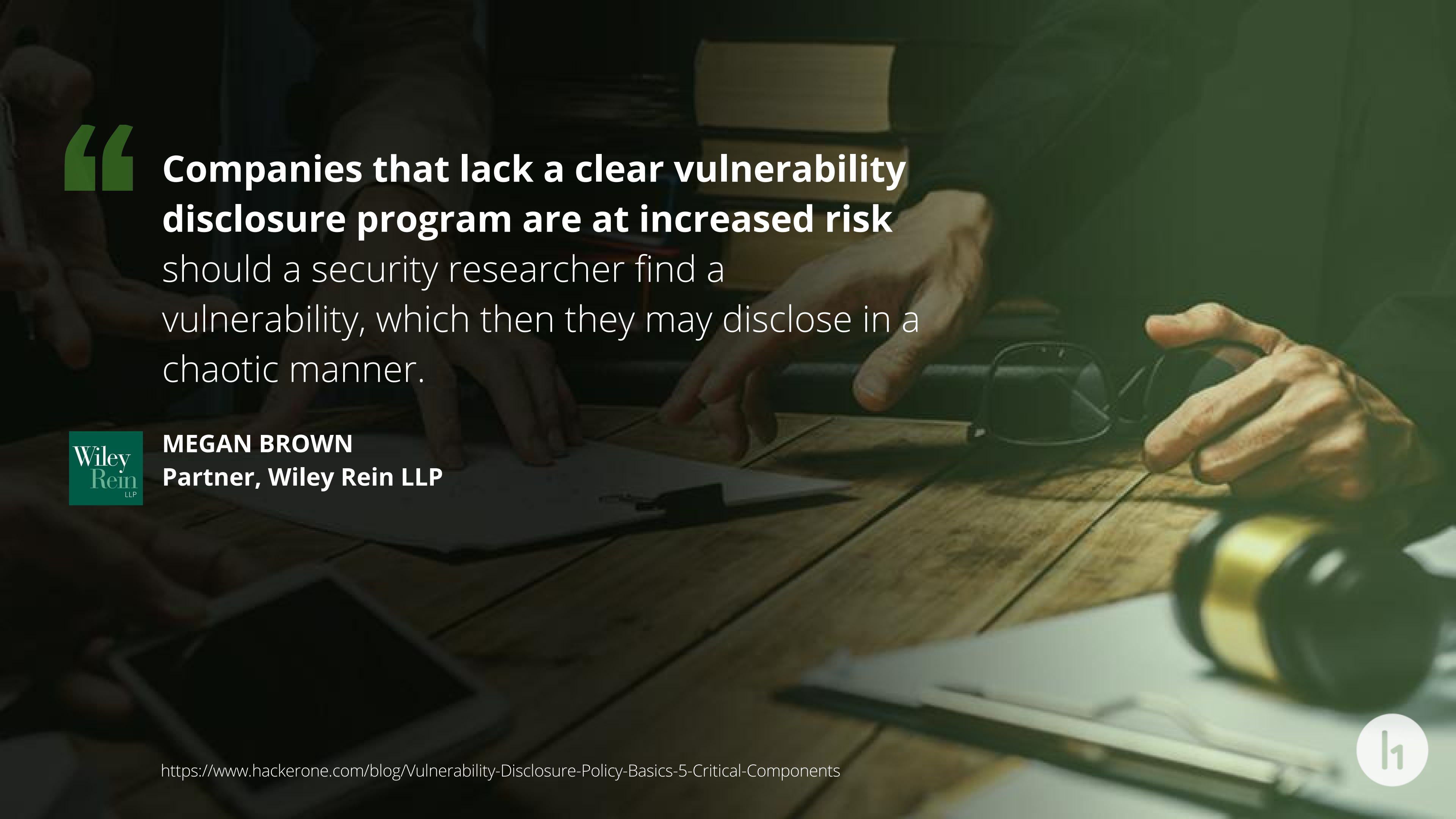
https://www.cnet.com/roadshow/news/general-motors-cybersecurity/

> **Vulnerability disclosure has long been an open, important issue in cybersecurity.** Companies need a strategy to deal with flawed software, systems, and configurations—especially when the issues are first discovered by a third party. Without a strategy, for example, companies sometimes choose to threaten the third party with legal action rather than working together to fix the vulnerability.

ANGELA SIMPSON

Deputy Assistant Secretary for Communications and Information, National Telecommunications and Information Administration

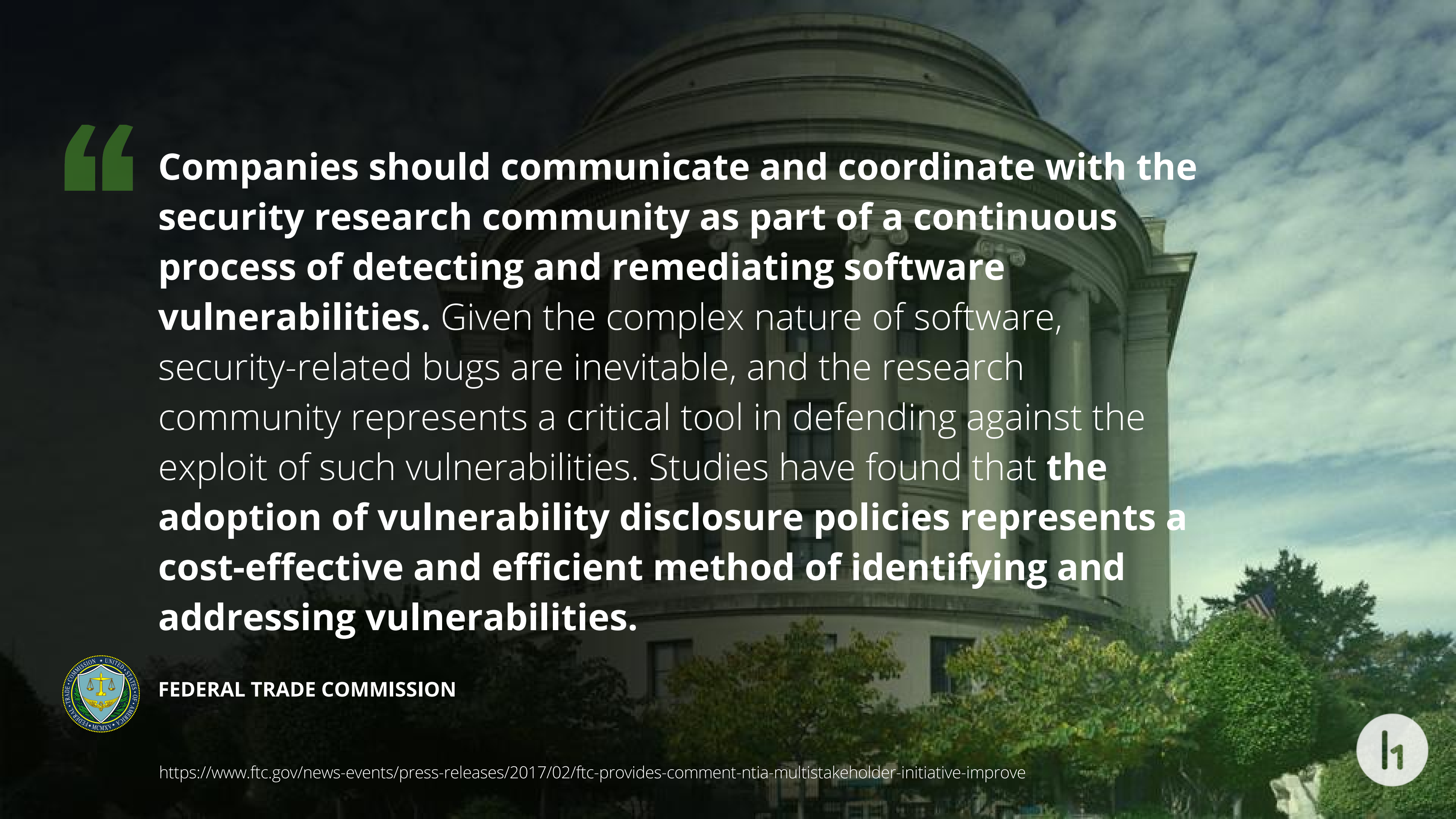
https://www.ntia.doc.gov/blog/2016/improving-cybersecurity-through-enhanced-vulnerability-disclosure



> **Companies that lack a clear vulnerability disclosure program are at increased risk** should a security researcher find a vulnerability, which then they may disclose in a chaotic manner.

MEGAN BROWN
Partner, Wiley Rein LLP

https://www.hackerone.com/blog/Vulnerability-Disclosure-Policy-Basics-5-Critical-Components



“ **Companies should communicate and coordinate with the security research community as part of a continuous process of detecting and remediating software vulnerabilities.** Given the complex nature of software, security-related bugs are inevitable, and the research community represents a critical tool in defending against the exploit of such vulnerabilities. Studies have found that **the adoption of vulnerability disclosure policies represents a cost-effective and efficient method of identifying and addressing vulnerabilities.**

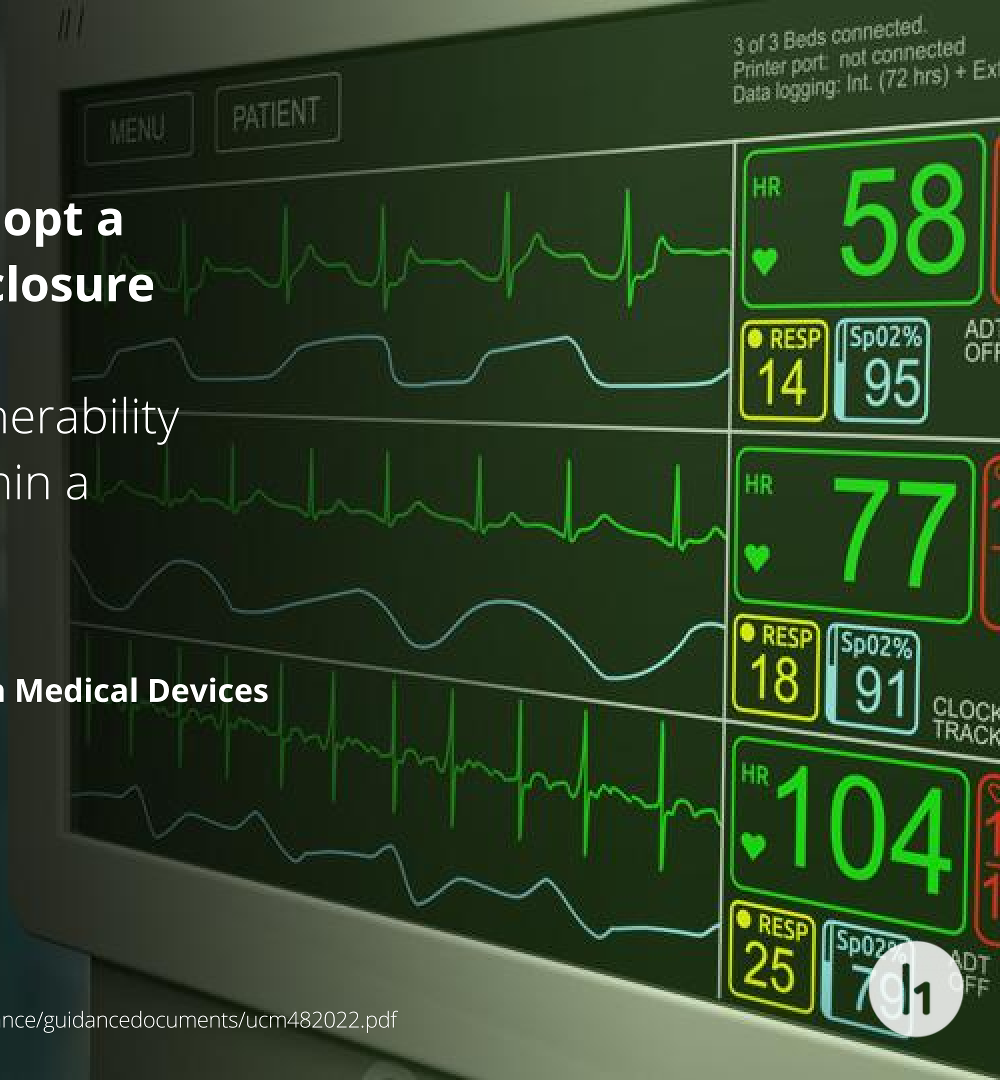
FEDERAL TRADE COMMISSION

https://www.ftc.gov/news-events/press-releases/2017/02/ftc-provides-comment-ntia-multistakeholder-initiative-improve

> I think a disclosure program, and going a step further, a bug bounty program, are tools available. In the right circumstances, I like those tools.

NICK RITTER
VP Product Security, General Electric

https://www.linkedin.com/feed/update/urn:li:activity:6311910907593191424/



> **Manufacturers should also adopt a coordinated vulnerability disclosure policy** and practice that includes acknowledging receipt of the vulnerability to the vulnerability submitter within a specified time frame.

U.S. FOOD AND DRUG ADMINISTRATION
Postmarket Management of Cybersecurity in Medical Devices

FDA U.S. FOOD & DRUG ADMINISTRATION

https://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm482022.pdf

> For those responsible for implementing the (Coordinated Vulnerability Disclosure) process, **defining a disclosure policy is an important first step.** A well-defined policy makes it clear what other participants in the CVD process can expect when they engage with you and establishes good relationships between finders, reporters, vendors, coordinators, and other stakeholders.

THE CERT® GUIDE TO COORDINATED VULNERABILITY DISCLOSURE
CERT Division of the Software Engineering Institute

https://resources.sei.cmu.edu/asset_files/SpecialReport/2017_003_001_503340.pdf

> **For the first time, anyone who identifies a security issue on a DoD website will have clear guidance on how to disclose that vulnerability in a safe, secure, and legal way.** This policy is the first of its kind for the Department.

ASH CARTER

Former Secretary of Defense, U.S. Department of Defense

https://medium.com/@SecDef/building-on-the-lessons-learned-from-hacking-the-pentagon-b5b58548b6a9

> This bill is designed to **let researchers look for critical vulnerabilities in devices purchased by the government without fear of prosecution** or being dragged to court by an irritated company.

SENATOR RON WYDEN (D-OR)
United States Senate

https://www.warner.senate.gov/public/index.cfm/2017/8/enators-introduce-bipartisan-legislation-to-improve-cybersecurity-of-internet-of-things-iot-devices

> Signatories of the Manifesto **acknowledge the importance to engage with researchers and the hacker community in the reporting of vulnerabilities** in their systems, so weaknesses can be detected and fixed in an early stage.

MANIFESTO ON COORDINATED VULNERABILITY DISCLOSURE
Global Forum on Cyber Expertise

GFCE
Global Forum on Cyber Expertise

https://www.thegfce.com/news/news/2016/05/12/launch-manifesto-on-responsible-disclosure

> Identifying and fixing vulnerabilities is therefore crucial, and the process of disclosing vulnerabilities is a vital component that cannot be underestimated.

GOOD PRACTICE GUIDE ON VULNERABILITY DISCLOSURE
European Union Agency for Network and Information Security

enisa

https://www.enisa.europa.eu/publications/vulnerability-disclosure

> Organisations will remain primarily responsible for the security of their information systems and (software) products, but **there has to be a quick and efficient response to reports in order to resolve vulnerabilities** and arrangements have to be made concerning any disclosure and information to other parties.
>
> Responsible disclosure thus concerns the actions of both the reporter and the organisation. **Specifically, this means that an organisation publicly endorses the responsible disclosure policy.**

GUIDELINE FOR RESPONSIBLE DISCLOSURE OF IT VULNERABILITIES
Ministry of Justice and Security, Government of the Netherlands

https://www.government.nl/latest/news/2013/01/03/guideline-for-responsible-disclosure-of-it-vulnerabilities

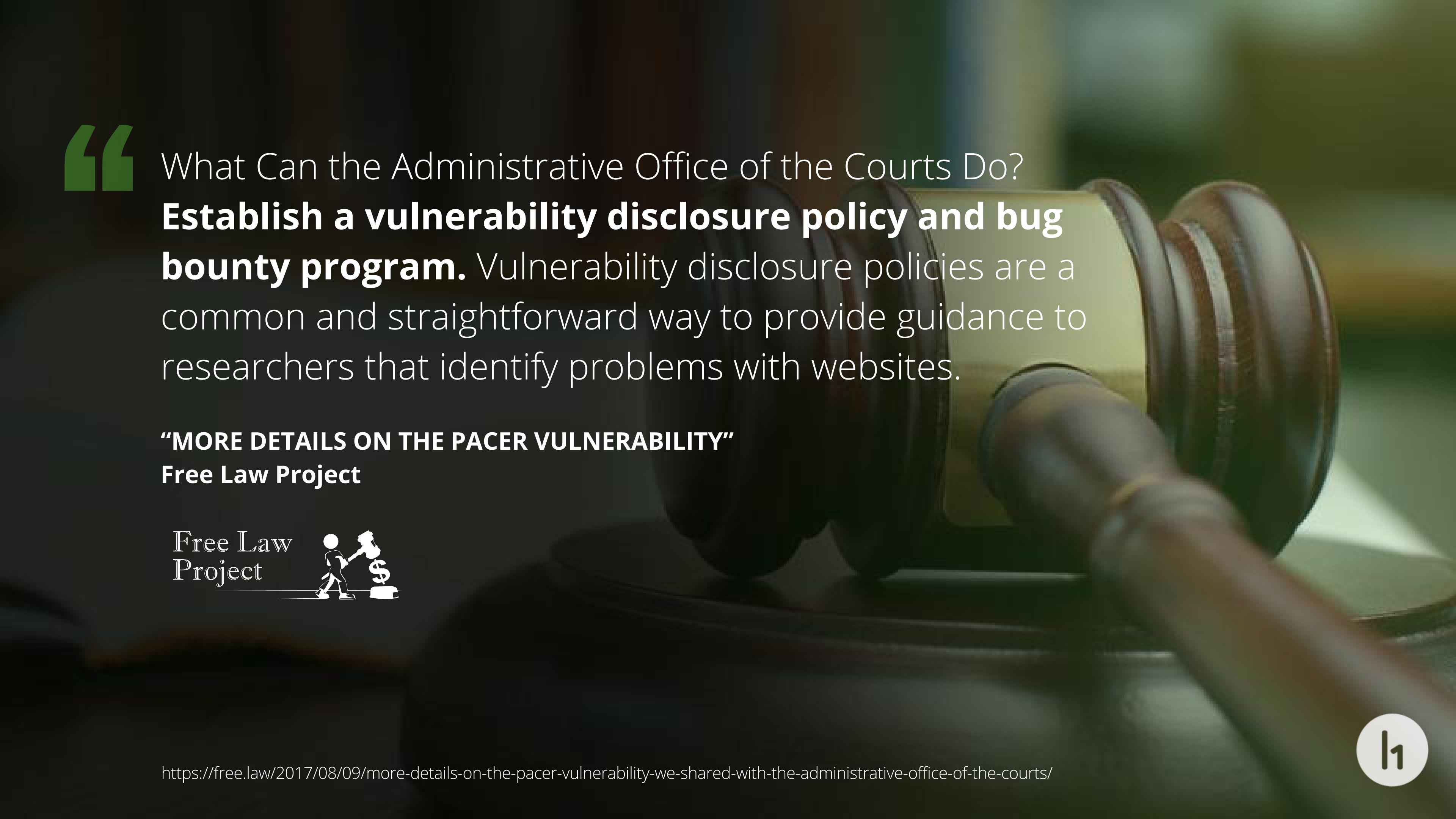
> We need to move to a world…where all **companies providing internet services and devices adhere to a vulnerability disclosure policy.**

JULIAN KING

Security Union Commissioner, European Commission

European
Commission

http://www.computerweekly.com/news/450427879/Euro-commissioner-calls-for-more-collaboration-on-cyber-security

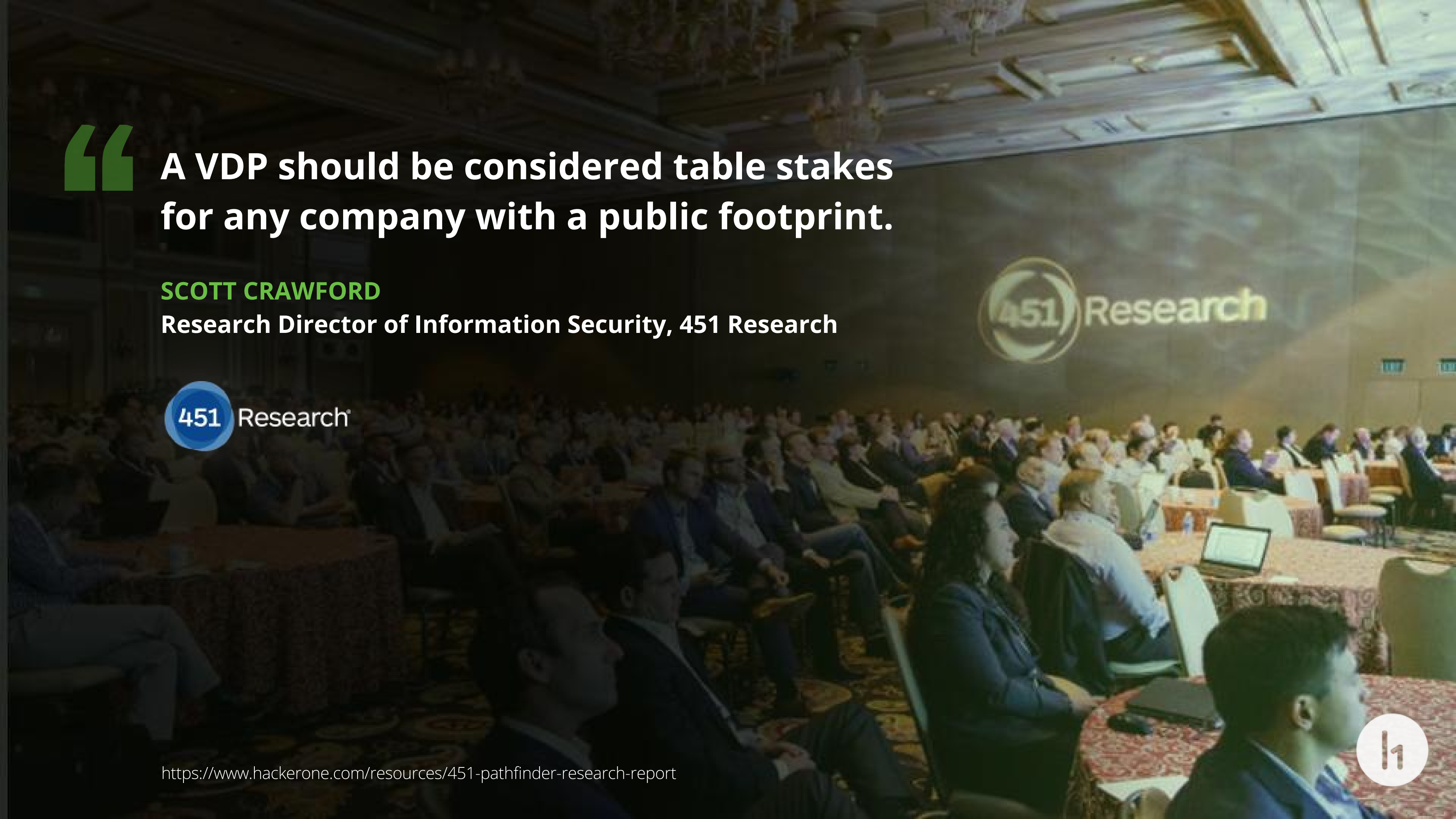


What Can the Administrative Office of the Courts Do? **Establish a vulnerability disclosure policy and bug bounty program.** Vulnerability disclosure policies are a common and straightforward way to provide guidance to researchers that identify problems with websites.

“MORE DETAILS ON THE PACER VULNERABILITY”
Free Law Project

Free Law
Project

https://free.law/2017/08/09/more-details-on-the-pacer-vulnerability-we-shared-with-the-administrative-office-of-the-courts/



> **A VDP should be considered table stakes for any company with a public footprint.**

SCOTT CRAWFORD
Research Director of Information Security, 451 Research

451 Research

https://www.hackerone.com/resources/451-pathfinder-research-report

5 Critical Components for Every VDP

Promise
Demonstrate a clear, good faith commitment to customers and other stakeholders potentially impacted by security vulnerabilities.

Scope
Indicate what properties, products, and vulnerability types are covered.

"Safe Harbor"
Assures that reporters of good faith will not be unduly penalized.

Process
The process finders use to report vulnerabilities.

Preferences
A living document that sets expectations for preferences and priorities regarding how reports will be evaluated.

Vulnerability Disclosure Policy Basics:

5 Critical Components

hackerone

DOWNLOAD THE FREE EBOOK

To learn more about generating your own VDP, download our "Vulnerability Disclosure Policy Basics" ebook. It details each of these 5 critical components, gives examples of text from real VDPs, and provides recommendations from pioneering organizations.