

## Ransomware, Hacking + Emerging Threats

---

### News

#### **Equifax Confirms Apache Struts Security Flaw It Failed to Patch Is to Blame for Hack**

Zack Whittaker | Sep 14

*ZDNet* - Equifax has confirmed that a web server vulnerability in Apache Struts that it failed to patch months ago was to blame for the data breach that affected 143 million consumers. [Read More](#)

#### **Equifax and the UK — What's Going On?**

Rory Cellan-Jones | Sep 14

*BBC* - On Friday, the UK's data protection regulator, the Information Commissioner's Office, put out a statement calling on Equifax to "alert affected UK customers at the earliest opportunity." We have sent a number of emails, but six days on, have received no replies about the UK situation. [Read More](#)

#### **Hackers' Latest Weapon: Cyber Extortion**

Robert McMillan | Sep 13

*The Wall Street Journal* - Instead of simply stealing passwords or credit-card data, or locking access to victims' systems as with ransomware, extortionist hackers try to unearth corporate secrets that they then threaten to make public if victims don't pay. [Read More](#)

#### **China Beefs up Cyber Defenses With Centralized Threat Database**

Cate Cadell | Sep 13

*Reuters* - China said on Wednesday it will create a national data repository for information on cyber attacks and require telecom firms, Internet companies and domain name providers to report threats to it. [Read More](#)

#### **US Official: American Companies Avoided Government Help When WannaCry, NotPetya Hit**

Chris Bing | Sep 13

*CyberScoop* - A top Department of Homeland Security official says the US government was unable to fully measure the scale and impact of two recent ransomware outbreaks, dubbed WannaCry and NotPetya, due to a lack of private sector engagement. [Read More](#)

#### **What Happens if a Cop Forces You to Unlock Your iPhone X With Your Face?**

Brian Fung | Sep 13

*The Washington Post* - For all intents and purposes, Face ID works just like its predecessor, Touch ID. The only difference is that instead of scanning your fingerprint, the iPhone X scans your face. But the introduction of Face ID also instantly led to questions among civil liberties experts, who say the technology raises the risk of abuse. [Read More](#)

#### **Hackers of All Stripes Set Sights on Shipping Industry**

Rhea Siers | Sep 12

*The Cipher Brief* - Recent fatal accidents involving two vessels in the US Seventh Fleet led to a spate of speculation about whether somehow the navigation in these ships was compromised by a cyber intrusion. [Read More](#)

## Legal + Market Intelligence

### **Deception: A Convincing New Approach to Cyber Defense**

Ofer Israeli | Sep 12

*Illusive Networks* - How defenders in a US national security agency capture-the-flag exercise used an endless stream of false data across the network to thwart attackers and contain damage. [Read More](#)

### **Trouble in Paradise as Cyber Attackers Circumvent 2FA**

Markus Jakobsson | Sep 14

*Agari* - While two-factor authentication (2FA) is a big step above and beyond the use of traditional passwords, it is not infallible, and thinking so makes the risk of failure even greater. [Read More](#)

### **Web Application Attack Statistics: Q2 2017**

Positive Technologies Staff | Sep 14

*Positive Technologies* - Compared to the previous quarter, attackers became slightly less active. Web applications were hit by 300 to 800 attacks on average per day, dipping as low as 140 on the slowest day. The maximum number of attacks on a single company in a single day was 35,135, almost double the top value from the previous quarter. [Read More](#)

### **The Hunt for IoT: The Rise of Thingbots**

Sara Boddy | Sep 14

*F5 Labs* - IoT devices are becoming the cyber weapon delivery system of choice by today's botnet-building attackers. And, why not? There are literally billions of them in the world, most of which are readily accessible (via Telnet) and easily hacked (due to lack of security controls). [Read More](#)

## Data Governance

---

### News

#### **UK's Data Protection Bill Contains Exemptions**

Phil Muncaster | Sep 14

*Infosecurity Magazine* - The UK government today published a Data Protection Bill designed to enshrine the EU GDPR into domestic legislation to minimize disruption to businesses post-Brexit. [Read More](#)

#### **EU Plans More Robust Security to Shore up Cyber Defenses**

Julia Fioretti | Sep 13

*Reuters* - The European Union's executive proposed on Wednesday a common plan to coordinate the bloc's response in case of a large-scale attack and a cyber security emergency response fund. [Read More](#)

#### **Study Says Enterprises Waste \$300K Annually on Cybersecurity Education**

Security Magazine Staff | Sep 14

*Security Magazine* - Despite growing investment of time, capital and human resources to increase security education, users remain the weakest link in security, and user-introduced threats continue to rise. [Read More](#)

## Legal + Market Intelligence

### **Data Breach Preparedness: A Critical Risk Management Priority for Small and Mid-Sized Businesses**

Joseph J. Lazzarotti | Sep 13

*Jackson Lewis P.C.* - Strong IT safeguards are part of the solution, but not a silver bullet. Administrative and physical safeguards also are needed, such as access management policies, awareness training, equipment inventory, and vendor assessment and management programs. But even the best safeguards cannot prevent all breaches. Thus, SMBs need to be prepared for responding to the inevitable – that they will experience a data breach of some kind. [Read More](#)

### **Be Smart About Insurance for the Smart Grid: Coverage for Losses From Cyber Events—Part II**

Amy J. Spencer | Sep 14

*Blank Rome LLP* - Traditionally, third-party losses are covered by a company's commercial general liability (CGL) policy. To qualify for coverage under a CGL policy, the policyholder typically must be confronted with a claim for "bodily injury" to another person or "physical injury to tangible property" (collectively known as "Coverage A"), or with a claim for "personal and advertising injury" (injury arising out of certain enumerated offenses such as malicious prosecution or invasion of privacy) ("Coverage B"). Various disputes have arisen as to whether cyber-related losses fit within these coverages. [Read More](#)

### **The Importance of Benchmarking in Your Security Program**

Joshua Goldfarb | Sep 13

*IDRRA* - Of course, like any term used in the security field, there can be a bit of confusion around what the term benchmarking means. What I am referring to here is understanding how an organization's security architecture compares with those of its peers, how it compares to industry standards and best practices, and where different gaps and shortcomings exist that lower the overall security maturity of the organization. [Read More](#)