Ransomware, Hacking + Emerging Threats

News

Financial Services Sector the No. 1 Target of Cybercriminals
Kelly Sheridan | May 01
Dark Reading - Cybercriminals go where the money is. More attackers are launching attacks on financial services institutions, which saw an increase in breached records, vulnerability disclosures, and DDoS attacks via IoT botnets in 2016. Read More

This Elite Cybercrime Group Is Wreaking Havoc on the US Restaurant Industry
Chris Bing | May 03
CyberScoop - A sophisticated hacking group with suspected ties to cybercrime gangs operating in Eastern Europe is now actively targeting and breaching prominent brand-name restaurants in the U.S. Read More

Hackers Ran Through Holes in Swift's Network
Katy Burne | Apr 30
The Wall Street Journal - In the past year, a spate of cyberattacks has penetrated banks along Swift's less-defended perimeter, shaking confidence in the dominant network used by banks for cross-border transactions. While Swift diligently locked down that network's core, customers were left mostly responsible for their own security, creating an opportunity for hackers. Read More

As Cyber Warfare Turns 10, the West Risks Falling Behind
Peter Apps | May 04
Reuters - For the West, "cyber" remains a tightly defined concept, a matter of protecting nationally vital systems, keeping secrets or finding them out from potential enemies. For countries like Russia and China, however, it has become something much broader. Read More

Europe Pumps Out 50 Percent More Cybercrime Attacks Than US
Dawn Kawamoto | May 04
Dark Reading - Cybercrime attacks launched from Europe reached more than 50 million in the first quarter, double the volume coming out of the US, according to the ThreatMetrix Q1 Cybercrime Report. Read More

Behold, the Spear Phish That Just Might Be Good Enough to Hook You
Dan Goodin | May 02
Ars Technica - As demonstrated by the recent Carbanak campaigns, the social engineering that goes into the best attacks isn't something that will be detected by intuition or street smarts alone. Read More

Hackers Get Back to the Basics
Kaveh Waddell | Apr 28
The Atlantic - The rise in email-delivered attacks is a reflection of a pattern that Symantec's research team calls "living off the land." It's essentially a return to basics: Rather than hoarding complex "zero- days"—attacks that exploit security holes for which no patches currently exist—or coding web-based malware, hackers are turning to more straightforward methods. Read More

How a Fake Cyber Statistic Raced Through Washington
Joseph Marks | May 03
Nextgov - The statistic, typically attributed to the National Cyber Security Alliance, is that 60 percent of small

businesses that suffer a cyberattack will go out of business within six months. But it's completely erroneous. Read More

Legal + Market Intelligence

FBI Warns of Cyber Threat in Healthcare Sector
Craig Newman | May 02
Patterson Belknap Webb & Tyler LLP - The FBI is warning the healthcare sector of a new cyber threat. In a Notification issued last week, the FBI said that it is "aware of criminal actors who are actively targeting" protected healthcare information ("PHI") and other personally identifiable information ("PII") from medical facilities "to intimidate, harass, and blackmail business owners." Read More

Cyber Attack Protection Steps for Investment Firms
Kristen J. Mathews | May 01
Proskauer Rose LLP - An email "spear phishing" scam has targeted investment firms recently, attempting to lure their personnel into inadvertently revealing their email account credentials to criminal fraudsters, and making wire transfers to the criminal's account instead of the intended account. Read More

Data Governance

News

Passwords to Become Passé as More Firms Back Biometrics
Liz Skinner | May 02
InvestmentNews - Some firms will aim the technologies at advisers, giving them safer access to firm information and client data. Others will focus on putting the tools in clients' hands. Experts expect that once these systems prove to be easier and more secure, they'll become the norm. Read More

Making Sense of Cybersecurity Qualifications
Stacy Collett | May 03
CSO - IBM's cybersecurity division has hired nearly 2,000 professionals to its security team since 2015. Leaders recognize that the skills needed to succeed don't always come in the form of a traditional degree, but "the sheer volume of new certifications being created does pose challenges," says Diana Kelley, global executive security adviser. Read More

Legal + Market Intelligence

Other States Start to Follow New York Lead on Cybersecurity of Regulated Entities
Danya Ahmed | May 04
Sedgwick LLP - Other states are now starting to follow New York's lead in mandating at least some degree of cybersecurity assessment for entities subject to state regulatory oversight. Colorado, for example, scheduled a hearing on proposed regulations targeted at financial investment advisors. Read More

CFTC Among Regulators Demanding Cybersecurity Vigilance

Samantha Ettari | May 04

Kramer Levin Naftalis & Frankel LLP - While the Securities and Exchange Commission (SEC) has garnered significant attention for its increased efforts and focus on regulating and enforcing enhanced cybersecurity measures within the U.S. financial markets, the Commodity Futures Trading Commission (CFTC) has also taken extensive steps in this emerging area. Read More

Cybersecurity Disclosures: A How-To Guide

Christopher M. Achatz | May 01

Bryan Cave LLP - The SEC staff acknowledged in the Cybersecurity Disclosure Guidance that no existing disclosure requirement explicitly refers to cybersecurity risks and cyber incidents, but has made clear that there are a number of disclosure requirements that might impose an obligation on an issuer to disclose such risks and incidents. Read More

Appeal in Home Depot Data Breach Derivative Action Results in Settlement of Corporate Governance Claims

Kevin M. McGinty | May 02

Mintz Levin Cohn Ferris Glovsky and Popeo PC - Snatching victory of a sort from the jaws of defeat, shareholders who brought a derivative action alleging that the 2014 Home Depot data breach resulted from officers' and directors' breaches of fiduciary duties have reached a settlement of those claims. Read More

It Lurks in the Last Place You Look — Preventing (or at Least Mitigating) Employee Data Leakage

James A. Sherer | May 03

BakerHostetler - Outside hacking attacks grab headlines. Data breach concerns cause sleepless nights within the C-suite of many organizations. And ransomware strikes fear into companies without sound backup practices and true Information Governance programs. But a different (and sometimes more sinister) problem often goes undetected within the four walls of those same organizations' firewalls and barriers to entry. It's not radon. It's the issue of data compromise or "leakage," perpetrated by employees, to the tune of billions of dollars every year. Read More