Egnyte Report Reveals 28% of Americans Unaware of Cyberattacks

Egnyte, a leader in secure content collaboration and governance, has released its latest report titled Hacked and Exposed: What Business Leaders Need to Know About Cyber Threats. The report's findings highlight cybersecurity trends, with 28% of Americans going months without realizing they've been hacked, often targeting their financial accounts and leading to significant monetary losses.

According to a comprehensive survey of 1,301 U.S. heads of household, cybercriminals are utilizing increasingly sophisticated tactics to exploit security vulnerabilities. These tactics include phishing emails, weak passwords, and social engineering strategies.

Kris Lahiri, Chief Security Officer and Co-Founder of Egnyte, stated, "The report not only underscores the prevalence of cyberattacks but also the concern that many people remain unaware of breaches for an extended period. This delay allows hackers to compromise multiple accounts."

He emphasized the importance of reviewing and strengthening personal and professional security practices, such as diversifying passwords to reduce the risk of attacks.

The report also highlights the sectors most vulnerable to cyberattacks:

41% reported being financially hacked, making them the most vulnerable group in the study. 36% of individuals working in banking and finance experienced financial hacks, emphasizing the need for stronger cybersecurity.

31% of professionals were targeted by phishing and email-based attacks. Workers in office and healthcare settings also experienced high rates of cyberattacks, with 29% of office employees and 25% of healthcare workers reporting financial hacks.

Neil Jones, cybersecurity evangelist at Egnyte, remarked, “The findings regarding work location may surprise many. It’s often assumed that on-site offices provide better security. Still, our report suggests that organizations with remote workforces are more proactive in cybersecurity training, network security, and access control than those with only on-site employees.”

Adobe Acrobat Vulnerabilities Allow Remote Code Execution

Security researchers from Cisco Talos have discovered multiple vulnerabilities in Adobe Acrobat, potentially allowing attackers to execute arbitrary code or access sensitive information. These flaws primarily stem from issues in the software’s font handling functionality.

The identified vulnerabilities include out-of-bounds read flaws and a memory corruption issue, which could be exploited through maliciously crafted PDF files.

CVE-2025-27163 & CVE-2025-27164 may lead to sensitive information disclosure. Attackers could leverage these weaknesses to gain unauthorized access to system data.
CVE-2025-27158 is a memory corruption vulnerability caused by an uninitialized pointer in Adobe Acrobat’s font processing. If exploited, this flaw could allow an attacker to execute

arbitrary code.

The susceptibilities affect various versions of Adobe Acrobat, though specific impacted versions have not yet been disclosed in detail. If successfully exploited, these exposure could allow attackers to steal sensitive data from affected systems. It can remotely execute malicious code and gain unauthorized system access.

Given the widespread use of Adobe Acrobat for PDF management, these security issues pose a significant risk to individual users and businesses alike.

To protect against potential exploits, users and organizations should take immediate action. Adobe has released patches addressing these harms. Users are urged to apply the latest security updates promptly. Avoid opening PDF documents from untrusted or unknown sources. Implement endpoint security solutions and intrusion detection systems to mitigate exploitation risks.

Children and Teens’ Online Privacy Protection Act Reintroduced

On March 4, 2025, Senators Ed Markey (D-MA) and Bill Cassidy (R-LA) reintroduced the Children and Teens’ Online Privacy Protection Act (COPPA 2.0), aiming to enhance online privacy safeguards for minors.

COPPA 2.0 prohibits digital platforms from directing targeted ads at children and teenagers. This law requires companies to

limit the collection of personal data from minors and mandates the deletion of such data. It restricts internet companies from gathering data from users aged 13 to 16 without explicit permission.

Senator Markey has persistently championed this legislation since its initial introduction in 2011. In the previous Congress, COPPA 2.0 was incorporated into a broader children's online safety bill, which the Senate approved with a 91-3 vote in July. However, the House of Representatives did not proceed with a vote on the bill.

The reintroduction has garnered support from numerous children's advocacy groups, teacher unions, privacy organizations, and medical associations. Senator Cassidy emphasized the bill's significance: "COPPA 2.0 is the tool that will give parents the peace of mind they need and keep their children's personal information secure."

Advocates highlight the increasing surveillance of children across social media and gaming platforms, where companies collect data to track, profile, and influence young users. Katharina Kopp, deputy director of the Center for

Digital Democracy, noted, "Children's surveillance has only intensified across social media, gaming, and virtual spaces, where companies harvest data to track, profile, and manipulate young users."

The continuation of COPPA 2.0 underscores a continued legislative effort to strengthen online privacy protections for minors in the digital age.

CISA Warns of Exploited Flaws in Cisco, Microsoft, Hitachi & Progress

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) has added five security vulnerabilities affecting Cisco, Hitachi Vantara, Microsoft Windows, and Progress WhatsUp Gold to its Known Exploited Vulnerabilities (KEV) catalog. This action signals that these flaws are actively exploited in the wild, posing significant risks to affected systems.

One of the vulnerabilities, **CVE-2023-20118**, affects Cisco Small Business RV Series Routers. This command injection flaw exists in the router's web-based management interface, allowing authenticated remote attackers to gain root-level privileges and access sensitive data. Cisco has not provided a fix since these routers have reached their end-of-life status, leaving organizations vulnerable.

Two security flaws in the Hitachi Vantara Pentaho BA Server, **CVE-2022-43939** and **CVE-2022-43769**, have also been flagged. The first vulnerability arises from an authorization bypass issue, enabling attackers to access resources through non-canonical URL paths. The second flaw allows attackers to inject malicious Spring templates into configuration files, leading to arbitrary command execution. Both issues were addressed in security updates released in August 2024.

An older vulnerability, **CVE-2018-8639**, affecting Microsoft Windows Win32k, has resurfaced as an active threat. This flaw, which allows local privilege escalation through improper resource handling, was initially patched in December 2018 but is still targeted in modern attack campaigns.

Another high-risk vulnerability, **CVE-2024-4885**, affects

Progress WhatsUp Gold, a widely used network monitoring software. This path traversal vulnerability enables unauthenticated, remote attackers to execute arbitrary code on affected systems. The flaw was patched in June 2024 with version 2023.1.3, but ongoing exploitation attempts have been observed.

C**VE-2023-20118** is being leveraged to conscript vulnerable Cisco routers into a botnet called PolarEdge. At the same time, the exploitation of CVE-2024-4885 has been detected globally. Security researchers from the Shadowserver Foundation and GreyNoise report that attack attempts have originated from Hong Kong, Russia, Brazil, South Korea, and the United Kingdom.

CISA has identified active exploitation of vulnerabilities. To ensure their systems are safeguarded, they have mandated that Federal Civilian Executive Branch (FCEB) agencies implement mitigations by March 24, 2025. Organizations using affected products are strongly urged to take action. They should apply the latest patches or implement alternative security measures, which will help prevent potential attacks.

How Cybersecurity Fits into Your Compliance and Ethics Program

NewsCybersecurity wasn’t necessarily a significant issue for in-house counsel 10-15 years ago.

Goodwin Procter Hit by Data Breach Through Vendor

NewsGoodwin Procter LLP suffered a data breach after a vendor that it uses for large file transfers was hacked, according to an internal memo obtained by news outlets.

Zoom Reaches Settlement with FTC Over Misleading Security Practices

NewsThe Federal Trade Commission reached a settlement with Zoom to resolve allegations that the company engaged in misleading security practices.

Privileged Cybersecurity Investigations – A Checklist for Contracting with

Consultants

WebinarBlog post discussing a checklist for companies contracting with cybersecurity vendors and consultants.

DOJ Reached $46M Settlement with 5Dimes for Illegal Sports Betting

News5Dimes and the U.S. Department of Justice reached a $46.8 million settlement of an investigation into illegal US sports betting operations, as well as money laundering and wire fraud.

Facebook Brings Suit against Developers of a Browser Extension That Harvested User Data

NewsFacebook brought suit against two marketing analytics firms alleging the defendants developed and distributed malicious Chrome browser extensions that were essentially designed to scrape users’ data from various social media platforms.

State Gets $1.9 Million as Share of Data Breach Settlement

NewsKentucky will receive more than $1.9 million as its share of a settlement with a company over a data security breach that compromised the personal information of 78.8 million Americans.

Fake Websites for Four Biglaw Firms Might Have Been Created to Get Deal Information

News

Fake websites for four large law firms created in 2008 might have been part of an attempt to get insider information on pending Wall Street deals, according to newly declassified FBI documents.

Facebook's $550 Million Settlement In Facial Recognition Case Is Not Enough

News

U.S. District Judge James Donato of California, who is overseeing the case, says that payout is woefully inadequate.

Centre for Information Policy Leadership at Hunton Andrews Kurth Issues Report on Accountability in Data Privacy

Insight

The Centre for Information Policy Leadership at Hunton Andrews Kurth has issued a report on how leading companies have implemented robust privacy programs and accountability controls.

Texas Courts Hit by Ransomware Attack

News

Texas courts shut down websites and disabled servers late last week in response to a ransomware attack, the Office of Court Administration announced.

Law Firm Representing Lady Gaga, Madonna, Bruce Springsteen, Others Suffers Major Data Breach

News

Grubman Shire Meiselas & Sacks, a large media and entertainment law firm, appears to have been the victim of a cyberattack that resulted in the theft of an enormous batch of private information on dozens of celebrities, according to a data security researcher.

Ten Tips on Handling a

Virtual Evidentiary Hearing Before a Regulatory Agency

News

“A virtual hearing can be challenging for any regulatory lawyer. It requires relying on technology more than ever to advocate for clients. It can feel like talking to an empty room, even if you’re on camera.

Equifax To Pay Mass. $18.2 Million In Settlement, AG Healey Announces

News

Equifax will pay Massachusetts $18.2 million and change its security practices as part of a settlement between the credit reporting agency and the state stemming from a major 2017 data breach, Attorney General Maura Healey announced Friday.

Protecting Your Sensitive Information While Using

Virtual Meeting Platforms

News

Over the last several weeks, virtual meetings have become the new normal for many businesses. Improvements in the technology now mean that virtual meetings have a similar look and feel as in-person meetings.

Jeep Drivers’ Claims Come to a Screeching Halt

News

A five-year legal battle between three certified classes of Jeep Cherokee drivers and Fiat Chrysler came to a sudden end, when a federal judge in the Southern District of Illinois held that allegations that the vehicles were vulnerable to cyber-attacks did not give plaintiffs standing to sue under Article III of the Constitution.