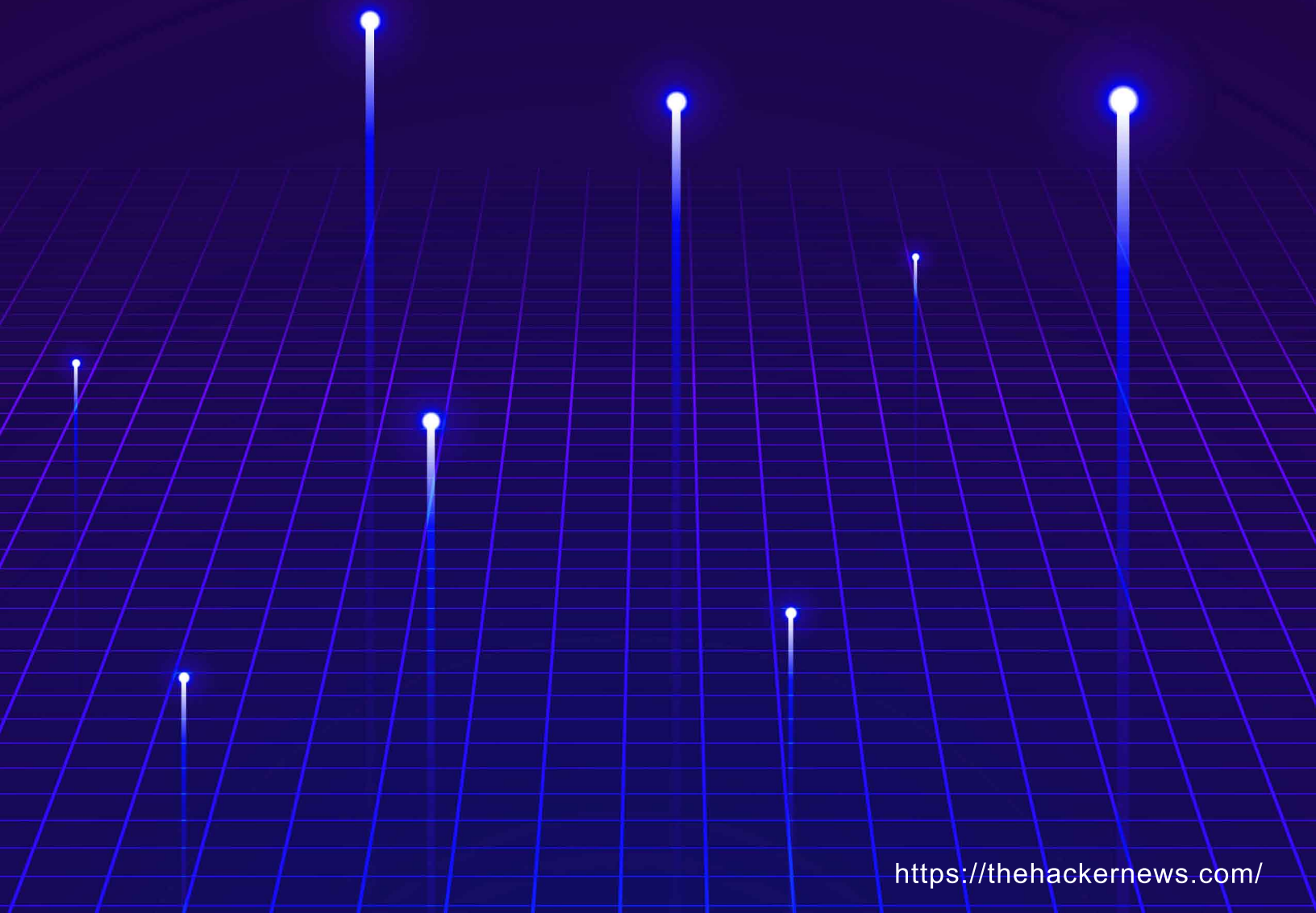
The Hacker News

Cyber Security Predictions

2020



https://thehackernews.com/

Top 5 Cybersecurity and Cybercrime Predictions for 2020

We distilled 30 independent reports dedicated to cybersecurity and cybercrime predictions for 2020 and compiled the top 5 most interesting findings and projections in this post.

1.) Compliance fatigue will spread among security professionals

Being a source of ongoing controversy and debate, the California Consumer Privacy Act (CCPA) was finalized on 11th January 1, 2019.

Driven by laudable objectives to protect Californians' personal data, prevent its misuse or unconsented usage by unscrupulous entities, the law imposes formidable monetary penalties of up to $7,500 per intentional violation and $2,500 per unintentional violation.

The Act is enforceable against organizations that process or handle personal data of California residents, regardless of the geographical location of the former. Akin to the EU GDPR, data subjects are empowered with a bundle of rights to control their personal data and its eventual usage.

The pitfall is that if every US state introduces its own state privacy law, one will have to comply with over 50 overlappings and sometimes incompatibly contradictive regulations only on the US territory or otherwise face harsh financial penalties or even criminal prosecution.

Exacerbated by the mushrooming regional, national, and transnational regulations, 2020 may become a year when cybersecurity compliance will erode and start its rapid downfall. In light of the slow judicial system on one side, and insufficient cybersecurity skills and scanty budgets on another, cybersecurity professionals may start flatly disregarding the wide spectrum of superfluous regulations.

2.) Third-party data breaches will dominate the threat landscape

Supply chain attacks are up 78% in 2019, says Symantec. Competitive and successful businesses are usually distinguished by a high level of proficiency and specialization, concentrating all available resources to attain excellence in a particular market to outpace competitors.

Hence, they outsource most of their secondary business processes to skilled suppliers and experienced third-parties, thereby reducing costs, increasing quality, and accelerating delivery.

Sadly, suppliers also operate in turbulent and highly-competitive global markets and thus can rarely afford a decent level of cybersecurity and data protection for their clients.

IBM says the average time to identify a breach in 2019 was as high as 206 days. Still, even worse, such attacks are infrequently detected both due to their sophistication and lack of skills amid the victims, eventually being suddenly reported by security researchers or journalists and flabbergasting the data owners.

Cybercriminals are well aware of this low-hanging fruit and will continue to purposely target this weakest link to get your data, trade secrets, and intellectual property.

3.) External attack surface will continue to expand without control

61% of organizations have experienced an IoT security incident in 2019, according to CSO Online by IDG. The global proliferation of IoT and connected devices, usage of public cloud, PaaS, and IaaS greatly facilitates business and enables rapid growth. Concomitant, and often unnoticed, is the increase in an organization's external attack surface.

Put it simply; an external attack surface is composed of all your digital assets (aka IT assets) that attackers can access from the Internet and attribute to your organization.

Traditional digital assets, such as network or web servers, are usually well inventoried, but RESTful API and web services, hybrid cloud applications, and business-critical data hosted on external platforms - are just a few examples of mushrooming digital assets of a modern-day attack surface that remain unattended.

As you cannot protect what you don't know, the vast proportion of these digital assets are not properly maintained, monitored, or protected in any manner.

The situation is exacerbated by rogue mobile apps, fraudulent, phishing, and squatting websites, detectable by properly implemented domain security monitoring that now starts paving its road to popularity among cybersecurity professionals.

In summary, as organizations upgrade their IT and leave behind a trail of obscure digital unknowns, whether in-house or external, the easier and faster it is to break in.

4.) Cloud misconfigurations will expose billions of records

Forbes says that 83% of enterprise workloads will move to the cloud by 2020. Unfortunately, the steady growth of the cloud for data storage and processing widely outruns requisite security skills and adequate training among IT personnel in charge of cloud infrastructure.

Gartner reports that around 95% of cloud security failures result as a fault of the customer, not vendors of public cloud infrastructure.

Unsurprisingly, a substantial part of significant data leaks in 2019 stems from misconfigured cloud storage, exposing the crown Jewels of the largest tech companies and financial institutions.

In July 2019, the world media reported a breach of Capital One, being presumably the largest data breach within the US financial sector and affecting approximately 100 million individuals in the United States and 6 million in Canada.

Reportedly, the attacker exploited a misconfigured AWS S3 bucket to download extremely sensitive data left unattended.

While Capital One estimated only its direct losses stemming from the breach to attain $150 million, the FBI later disclosed that as many as 30 other organizations could have been compromised using the same AWS misconfiguration.

Foreseeably, in 2020, cloud security incidents will stay atop of data breach root causes.

5.) Password re-use and phishing attacks will skyrocket

Just for the world's largest companies from the Fortune 500 list, one may ferret out over 21 million of valid credentials exposed in the Dark Web in 2019, says ImmuniWeb.

Cybercriminals prefer rapid and riskless raids to time-consuming APT attacks, costly 0days, or chained exploitation of sophisticated vulnerabilities in SAP.

Even if many organizations finally managed to implement a consumable Identity and Access Management (IAM) systems, with strong password policies, MFA, and continuous monitoring for anomalies, few external systems are included in the safeguarded scope.

Such grey-zone systems range from SaaS CRM and ERP to elastic public cloud platforms.

Even if the passwords found or purchased by the attackers on the Dark Web are invalid, they provide a great wealth of ideas for ingenious social engineering campaigns, facilitate phishing and smart brute-forcing attacks.

Frequently, these attacks, being at first sight quite primitive from a technical standpoint, demonstrate astonishing efficiency and relentlessly undermine and decollate the organization's cybersecurity resilience efforts.