

reflecJiz



Top 2020
Cybersecurity Events:
**Key Takeaways
for 2021**



2020 will always be remembered as the year of COVID-19, but it was also a big one for digitalization across multiple sectors. eCommerce websites, along with banking, insurance, healthcare, and other eService platforms, scaled up exponentially due to the new circumstances. Unfortunately, the same cannot be said about third-party application security. These external web applications are creating a plethora of security and compliance risks that kept re-surfacing in 2020.

Let's take a closer look at the biggest cybersecurity events and what we can learn from them.

Cybersecurity in the United States - CCPA, 23 NYCRR 500, HIPAA, SOX, CDPA, and the List Keeps Growing

CCPA, also known as the California Consumers Protection Act 2018, was the biggest US privacy law to officially go live last year. Multiple eCommerce sites and eService providers are already facing the heat from regulators for mishandling private data and mismanagement of third-party applications. Go ahead and follow Lexology's CCPA tracker to stay in the loop - [Click Here](#).

The rapid digitalization of eCommerce and other online services in the United States means that all websites will now be closely monitored and regulated.

Takeaway No.1:

CCPA guidelines state that businesses can pay anywhere from \$2500 to \$7500 per violation (stolen record). Now's the time to invest in security.



Related: [Achieving CCPA with Third-Party App Security](#)

The financial sector also needs to take note. The State of New York enforced 23 NYCRR 500, a strict set of rules to ensure that New York based financial and insurance companies are taking a proactive approach when it comes to protecting financial data. First American Title Insurance Company (First American) is already facing legal action for [violating 23 NYCRR 500](#).

Takeaway No.2:

US-based financial businesses need to prioritize data privacy by enforcing the latest compliance standards.



This is just the tip of the iceberg. Healthcare companies and insurers already need to comply with the Health Insurance Portability and Accounting Act (HIPAA), which governs the management of Personal Health Information (PHI). Also, the State of Virginia has now announced its own version of privacy laws, the CDPA (Consumer Data Protection Act), which takes effect January 1, 2023.



Takeaway No.3:

Data privacy laws have arrived in the United States.
You have to prioritize third-party security to stay out of trouble.



The SolarWinds Hack

The SolarWinds case is surely the biggest hack of 2020 and arguably the most significant one of the decade. This mega-breach showed how vulnerable companies become due to unmonitored or untracked third-parties, which can be exploited to initiate devastating supply-chain attacks. This is very much relevant also to websites offering online shopping or financial services.

Takeaway No.4:

Supply-chain attacks are expensive. Cleaning up the damages caused by the SolarWinds hack will cost over 100 million USD.



Microsoft, Cisco, Intel, Deloitte, and even some parts of the Pentagon were affected by this cyberattack, which is expected to create ripples in 2021 and beyond. In an ironic turn of events, it was revealed that even cybersecurity giant FireEye fell prey to this vicious attack, which was later found to be a politically motivated operation initiated by Russian hackers.

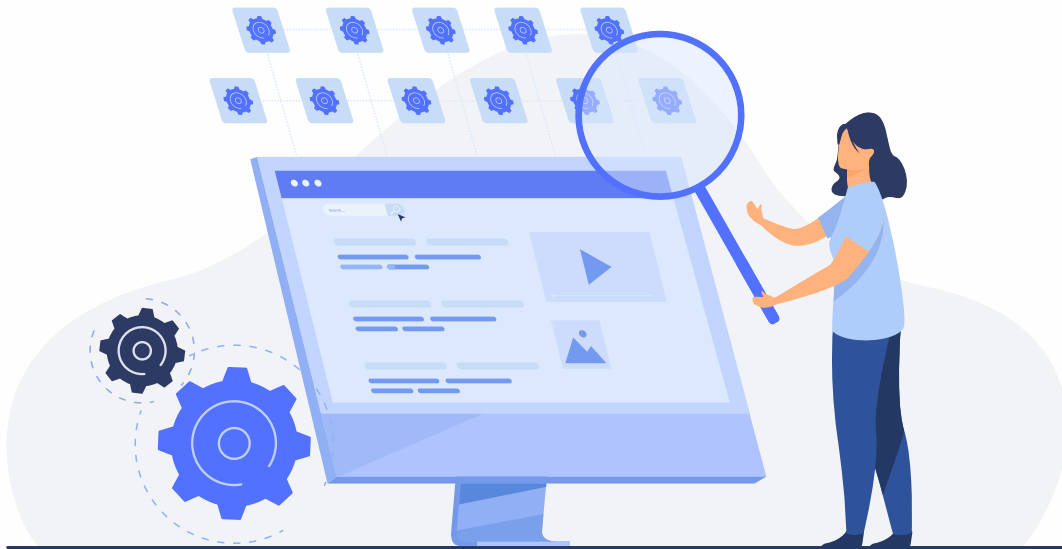
Takeaway No.5:

Third-party application vulnerabilities need to be taken seriously as they create multiple security blind spots in your ecosystem.

The rapid digitalization of 2020 (and the last decade in general) has led to companies scaling up fast. More and more websites are now implementing third-party solutions to address their sales, marketing, IT, and management requirements. This shift is definitely boosting productivity, but is also creating undetected security risks and regulatory concerns that can prove to be costly.

Takeaway No.6:

As per a recent study conducted by the Reflectiz team, websites are now using over 50 third-party web applications on average.



Related: [In Retrospect: The SolarWinds Attack](#)

Web-Skimming and Magecart Events

COVID-19 wasn't the only pandemic the world had to deal with in 2020. A Dutch cybersecurity research team exposed [a malicious Magecart script](#) that can manipulate popular eCommerce platforms such as Shopify, Zencart, Woocommerce, and BigCommerce. This finding shook the security industry, as there are thousands of websites that are based on these platforms.

That's not all. [Social media sharing buttons](#) used on these websites were also found to be possible attack vectors. The root cause - third-party applications. All victims eventually failed to implement a layered security approach that involved risk assessment, ongoing monitoring, and real-time mitigation of security risks created by external third-parties running on websites.

Takeaway No.7:

Magecart is evolving, with hackers finding new ways to exploit eCommerce websites. Even JPG files are being manipulated.

Looking to join the fight against Magecart and Web-Skimming? Join our LinkedIn group and share your knowledge with the cybersecurity community:

[Web-Skimming and Magecart Cyber Attacks](#)



There were multiple Web-Skimming cases last year. The Tokyo Olympics, a global event that was eventually postponed due to the COVID-19 pandemic, also attracted cybercriminals. A major ticket reseller's website was found to contain [malicious JavaScript code](#). We also have to mention the infamous [Ticketmaster UK hack](#), which kept making headlines in 2020 due to its legal implications.

Takeaway No.8:

Magecart and Web-Skimming are not exclusive to eCommerce websites. All websites offering eServices are now potential targets.

[Camera retailers](#), [school management platforms](#), [cosmetic online shops](#), and [donation sites](#) were also not spared by cybercriminals in 2020. This has led to the clear conclusion that third-party application security is now mandatory on all websites offering eServices. CISOs and security teams need to take control of third-parties and monitor dependencies at all times.

Takeaway No.9:

Web-Skimming is a global threat that also needs to be addressed with a robust third-party monitoring solution for a holistic 360 view.

Are You Prepared for the Challenges of 2021?

There are no shortcuts when it comes to cybersecurity. Solutions like Web Applications Firewalls (WAFs), tools like Content Security Policies (CSPs), and Penetration (Pen) Testing services are effective to some extent. But the dynamic nature of third-party applications requires a rethinking of how websites need to be safeguarded. The answer is simple - third-party application governance.



Takeaway No.10:

The CSP is simply not enough, as it is tough to configure, has false-positive issues, and doesn't protect you from hacked trusted parties.



Web-Skimming and Magecart Events

2020 has shown us that third-parties are beneficial on many levels, but they also introduce risks and dependencies that are creating multiple attack vectors. Only a proactive approach that involves ongoing monitoring of third-parties and detection of unwanted dependencies can help you stay protected and eliminate risks like Web-Skimming (Magecart) and supply chain attacks.



You need to mitigate client-side risks before they happen, ideally with a good monitoring tool that is easy to install and requires little to no maintenance. Discovering and eliminating your security blind spots caused by third-parties apps is the only way to enforce the right security standards on your website.

Idan Cohen, CEO, Reflectiz

About Reflectiz

Reflectiz empowers digital businesses to make web applications safer by non-intrusively mitigating third-party risks without a single line of code.

Our advanced technology is designed to protect your website against client-side attacks and Magecart threat actors, form-jacking, GDPR/CCPA/23NYCRR500 violations, and data breaches.



Take Control of Your Third-Parties

Keep your website safe from third-party security threats and compliance risks?

REQUEST FREE RISK ANALYSIS