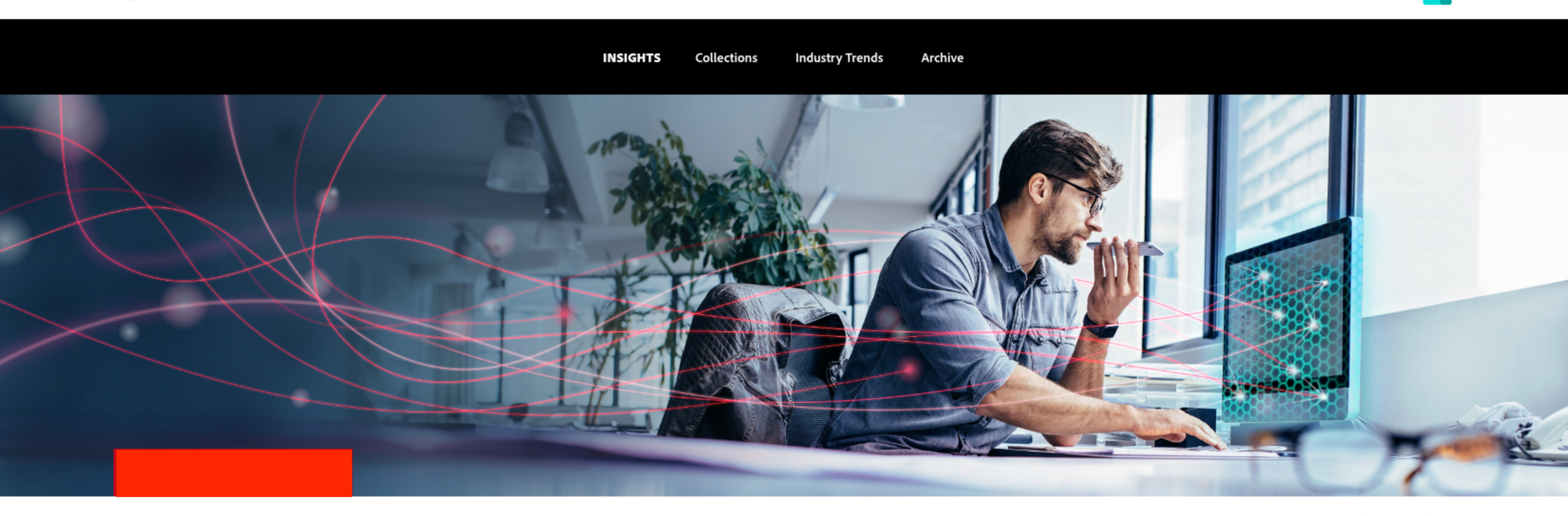


NOW READING
1 Market to me. Not my device.
NEXT UP
2 Head off 'sloppy growth' by first understanding your customers.
3 2017 Predictions: Digital Transformation, CX Top the List.
4 Use Offline Data to Improve the Customer Experience.

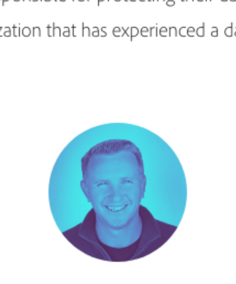
Secure your digital content. And your competitive edge.

"Site owners should immediately — and we mean right now — update their sites."

This is the advice one tech support site gave to readers when a highly critical security flaw threatened more than a million websites running on one of the most widely used open-source web content management systems. The flaw, which was upgraded to a 24/25 on the severity scale, allows attackers to run any code they want against the core component of a site's content management system (CMS), effectively taking over the site simply by visiting the URL. No logging in or authentication needed.

Breaches like these have been on the upswing, and so has the cost of downtime associated with them. A study by Information Technology Intelligence Consulting puts the average cost of downtime for most large enterprises at over $300,000 per hour. For some industries — finance, government, healthcare, manufacturing, media and communications, retail, transportation, and utilities — the average skyrockets to over $5 million per hour. Not to mention the hidden costs associated with recovering from a breach, like insurance premium increases and lost value of customer relationships.

And cybercrooks aren't just attacking your website. They're attacking the very way your company differentiates itself — the content and data at the heart of the customer experience. That means if your site goes down, so does your experience. According to Gemalto, 69 percent of consumers believe companies are primarily responsible for protecting their data, and 70 percent say they would stop doing business with an organization that has experienced a data breach.



"Your website is an important way to provide customers a view into your world, and what you have to offer. It's also a common way for bad actors to get into your CMS environment and cause problems."

Brad Bartholomew
Security Manager, Adobe Managed Services

With content and experience management named as the top strategic priority for organizations according to Econsultancy, it's time to secure your content, your data, and your competitive edge.

CMS: Your secure foundation for digital experiences.

Your IT team plays a primary role in reaching business objectives around creating, managing, and delivering the best customer experience. And your CMS is the digital foundation that helps you meet these objectives. That's why it's so important to keep it safe and secure.

Top priorities for IT professionals

44%	43%	38%
Security of business and customer data	Extensible digital platform for experience delivery	Better digital workflows using cloud-based tools

Source: Econsultancy and Adobe

Building a secure digital foundation also paves the way for innovation and scale, giving your team more time to focus on helping your business move forward.

Take this scenario. Due to a software vulnerability, the website of a high-profile retail bank suffered a DDoS attack, preventing customers from accessing online banking services. Although hackers didn't steal account numbers or money, the bank lost hundreds of thousands of dollars due to the downtime. The backlash from customers on social media also caused considerable damage to their brand and resulted in a loss of customer trust that the bank is still trying to rebuild.

Now imagine what would have happened if the bank's IT team had been working with an expert managed cloud service provider. The provider would have regularly patched their CMS, monitored their site around the clock, provided content encryption, performed backup and disaster recovery, and relied on cloud security certifications to keep their site — and their customers — safe. In short, the attack could have been avoided altogether, allowing the IT team to concentrate on getting their latest customer service mobile app to market faster, rather than cleaning up a security incident.

According to the Open Web Application Security Project (OWASP), your web applications are most at risk for threats like insufficient logging and monitoring, injection, broken authentication, sensitive data exposure, and broken access control. The list is long, but time is short. An effective security program includes vulnerability management as well as the ability to detect and respond to security issues in a timely manner.

With cyber risks like these right at your doorstep, getting your security house in order can't happen soon enough.

Seven must-have CMS security features.

1. Access control. Provide multiple levels of authentication (multi-factor authentication) to ensure your CMS environment is protected from simple username and password brute-force attempts.

2. Role-based access. To ensure your environment doesn't change without proper controls, implement role-based access, such as preventing developers from working in the production environment, or ensuring that content editors can't add JavaScript code to a page.

3. Auditing and monitoring. It's important to have near real-time access to changes happening in your CMS so that you can put checks in place and address issues accordingly.

4. Vulnerability management. Understand which vulnerabilities exist, monitor for them, assess potential impact, and respond depending on how critical the vulnerabilities are.

5. Intrusion detection. New hacks and vulnerabilities are always coming forward, so it's important to conduct periodic testing to find out if an attacker has broken in or compromised your system. The longer it takes to detect a breach, the more it will cost you.

6. Dedicated virtual private environments. One of the concerns about using the cloud and running in data centers is that you don't own and manage it. Virtual private cloud provides data isolation and separation, ensuring you don't expose your organization to the risk of data intermingling — often a challenge with public cloud.

7. DDoS protection. Anything that can bring your site down is a risk from a monetary and security perspective. DDoS protections detect increases in traffic and ensure that good traffic gets to the site while bad traffic is cut off before it attacks your environment.

Best practices: Keeping your CMS secure in the cloud.

From phishing attacks and drive-by downloads to suspicious logins and cryptocurrency miners, keeping your CMS secure in the cloud means more than patches and upgrades. Protect your site — and your customer experience — by taking the following actions.

Develop a strong security framework. A strong framework allows you to put processes and governance in place to protect your infrastructure, applications, and services. A security framework also helps you comply with industry best practices, standards, regulations, and certifications like PCI DSS, Safe Harbor, and SOX 404. Because it's not just about patching a server, it's about good change control, including training for personnel and users, a good hiring process, and a strong process for protecting your media.

Focus on data privacy and compliance. If your organization is in a high-regulatory industry like finance, government, or healthcare, make sure your cloud solution complies with FedRAMP, GLBA, HIPAA, ISO27001, SOC-2, and other required standards.

Document and protect your assets. Have a process in place to scan your assets to determine what ones you have and account for all of them. Then put the appropriate measures in place to secure those assets.

Keep an eye on your systems. Make sure you don't have any potentially unwanted programs installed. Implement strong systems for managing software, versioning, and acquisition of third-party software, including application and network scanning, security architecture review and penetration testing, and implementation of Intrusion Detection Systems (IDS) sensors to detect and alert security teams to unauthorized attempts to access your network.

Ensure viability. If you're working with a cloud service provider or other vendors, create a process to ensure you won't run out of server space, memory, or anything else that can bring your site down. You're only as secure as the systems your vendors are securing, and the systems and security they have in place.

Keep your CMS updated. Regularly review and apply the latest updates, including new features, bug fixes, and enhancements to ensure your deployment remains stable and secure. If you're working with a managed service provider, ensure they're patching guest operating systems (OS), your CMS software, and applications running on the cloud provider infrastructure.

Stick with your core capabilities. Keep your focus on strategic initiatives by working with a managed services provider to monitor potential threats and keep your CMS and cloud infrastructure management safe from malicious attacks.

IT: Clearing the path for innovation.

With higher customer expectations to fulfill, and more data than ever to manage, keeping risks down and innovation up is a delicate balancing act. But it's one that provides opportunities for IT to have a core role in transforming your business into one that competes — and wins — on customer experience. Whether it's crushing the latest security threat, or protecting customer privacy, it all starts with the right content management platform and the security practices to keep it strong. Because when you have a stable digital foundation, you can better concentrate on developing innovative ways to keep great experiences flowing and your business growing.

Adobe can help.

Recognized by Forrester and Gartner as a Leader in web content management, we understand the important role security plays in helping you deliver the personalized experiences your customers expect. Adobe Experience Manager Sites provides you with a complete digital foundation that enables you to quickly assemble insight-driven experiences while keeping customer data secure.

Learn more about how you can build a future-proof digital foundation with the cloud-based security of Adobe Experience Manager Sites.

Get the report

"2017 Reliability and Hourly Cost of Downtime Trends Survey," ITIC, 2017.

"Adobe Experience Cloud Security," Adobe, April 2017.

"Adobe Experience Manager Security Overview," Adobe, April 2018.

"Beneath the surface of a cyberattack," Deloitte, 2016.

Brad Bartholomew, Security Manager, Adobe Managed Services, personal interview, April 12, 2018.

Catalin Cimpanu, "Drupal Fixes Drupalgeddon2 Security Flaw That Allows Hackers to Take Over Sites," BleepingComputer, March 28, 2018.

"Data Breaches and Customer Loyalty 2017," Gemalto, 2017.

"OWASP Top 10 - 2017," The OWASP Foundation, 2017.

Prateek Vatash, "2018 Digital Trends in IT," Adobe and Econsultancy, 2018.