The Website Security Checklist

UpGuard

Introduction: Measuring Resilience

Incidence of breaches and data exposures are at an all time high. The fragility of digital business is being revealed under the additional stress of sophisticated attacks and complex operations. But cybersecurity spending is also at an all-time high. Organizations want to protect themselves and their data, but despite spending efforts, the problems have only worsened. Organizations need a way to measure not only their cyber risk, but the effectiveness of their efforts to remediate it. The value added by a cyber risk solution should be visible and quantified, so that spending in this area can be justified through data driven metrics.

UpGuard Cyber Risk assesses actual threat vectors, and provides a real time look at cyber risk posture for the entire organization, starting with third party and fourth party vendors, because their improvement, or worsening, should also be tracked— their risk is your risk. UpGuard also measures and tracks organizational risk for your websites and domains, offering guidance and best practices on how to shore up configurations and minimize the chance of breach. Each threat vector examined by UpGuard is recorded over time to create predictive trend lines for risk. Furthermore, UpGuard offers organizations and their vendors an opportunity to improve their security and operations, raising the bar across the board for cyber resilience.

Raising that bar means creating sustainable and secure internet-wide infrastructure capable of handling business operations, state functions, and other crucial aspects of society that have been digitized, without subjecting them-- and the information of every person— to unnecessary risk. By improving your posture and assessing your vendors on theirs, the entire digital ecosystem will grow more resilient, more agile, and better able to adapt to change while maintaining critical functions. What we need is not only a technology we can use, but a technology we can trust.

Man-in-the-Middle Attacks

Man-in-the-middle (MitM) attacks intercept data before it reaches the intended target. An online form, a password entered, even a website cookie can all be “sniffed” and stolen in transit without secure configurations.

Problems UpGuard Detects

- SSL not available
- Weak encryption algorithm
- Certificate about to expire
- HTTP Strict Transport Security not enforced
- Secure cookies not used

In the Real World

In July of 2017, the New York Times reported that among other types of attacks, hackers targeting nuclear facilities were using man-in-the-middle attacks to “redirect their victim’s internet traffic through their own machines.” In 2016, AdultFriendFinder suffered a massive data breach, including passwords that were cracked due to weak encryption algorithms. More than whether or not it’s there, the way encryption is used impacts every digital organization.

How to Fix It

Sitewide SSL

All websites should be encrypted with a Secure Sockets Layer (SSL) certificate from a trusted authority. To ensure that connections are encrypted, SSL should be sitewide and enforced, not a page-to-page choice that hands the client back and forth between encrypted and unencrypted connections. Every page should only be available on SSL. Information transmitted outside of SSL connections passes in plain text and can easily be intercepted by anyone willing to put the work in. A single form with sensitive information or password entry can compromise the entire site.

Strong Encryption Suites

Encrypting traffic doesn't do much good if the encryption used is weak or has known vulnerabilities. SSL certificates have evolved over time, and so have the encryption protocols they employ. When renewing certificates, always get the strongest encryption algorithms and keys whenever possible. Web servers should be configured to omit weak cipher suites and prioritize the use of the strongest first.

Certificate Expiry Process

By design, certificates expire after a short interval. The renewal process helps validate certificate ownership and also allows for encryption algorithms to be updated. Expired certificates break SSL encryption, and likely the entire website. An expired certificate injures an organization's reputation as well as crippling their web presence. The date the certificate expires is included among the data in the certificate, and as such can be monitored for expiry, with proactive notifications to kick off the renewal process. Because this is a regularly repeated process, it should be well-documented, with all questions answered before it's time to renew.

HTTP Strict Transport Security

HTTP Strict Transport Security (HSTS) ensures that browsers only communicate with a website over SSL. Non-SSL requests (http://) will be converted to SSL requests (https://) automatically. HSTS is enabled through a simple header or configuration directive (Linux, Windows). Failure to utilize this measure can result in a malicious actor redirecting a web user to a fraudulent site during the non-SSL and SSL handoff.

Secure Cookies

Secure cookies can only be transmitted across an encrypted connection. This prevents cookies with potentially sensitive information from being sniffed in transit between the server and the client. Secure cookies are enabled through a simple configuration directive in the web server. Failure to use secure cookies would allow a third party to intercept a cookie sent to a client and impersonate that client to the web server.

Vendor Recommendations

When a vendor is susceptible to MitM attacks, organizations should be more cautious about entering data on that vendor's website. Use unique passwords for their services, so that if a password is intercepted, it can't be reused for other purposes. Companies may choose to deliver their information through email or over the phone, rather than filling out forms online, to avoid the chance at exposure. Financial transactions, such as credit card payments, should not be made over websites vulnerable to this type of attack.

Exposed Server Information

By default, many websites announce information about themselves, including what kind of software they are powered by, and even what version of that software is being run. This narrows attack windows for malicious actors, now enabled to find specific exploits they know will work.

Problems UpGuard Detects

- ASP.NET version header exposed
- Server information header exposed
- X-powered-by header exposed

In the Real World

The way this vector is used goes like this:

1. Headers are gathered from company web servers
2. Attackers comb through headers to find old/outdated/vulnerable software
3. Known exploits for this software are used to attack the web server

OWASP found that running old software with known vulnerabilities was the number one cause of breach, followed closely by misconfiguration. Even established security companies can be compromised in this way. In January of 2017, Cellebrite, the Israeli mobile security company famous for its involvement in the FBI's hacking of an Apple iPhone, leaked over 900GB of data from an old server running on their network. Frontline production systems are usually well-secured. But an outlying server, perhaps a remainder from an upgrade operation, or a residual of an abandoned project, can be used to gain easy entry into an otherwise well protected environment.

How to Fix It

Exposed Headers

A simple true/false directive on the web server determines whether headers are obscured. It is recommended best practice to obscure these headers and present no identifying information to visitors. This is often not the default configuration, so many production servers still have these headers available, probably unknowingly.

Vendor Recommendations

When a vendor has exposed headers, it's usually because nobody knows they are exposed. Smaller vendors can be notified to the exposure, as best practices recommend obscuring them on all systems. If vulnerable software is being advertised, businesses should limit their interaction with the affected website as much as possible.

Cross-site Scripting Attacks

Cross-site scripting (XSS) is a method of attack that uses stored cookies to impersonate a user to a website. Cookies store authentication tokens; unprotected cookies can put those tokens into the hands of an attacker.

Problems UpGuard Detects

- HttpOnly cookies not used

In the Real World

Perhaps the most famous example of a cross-site scripting attack was the Samy Worm, an attack that used insecurities in the MySpace platform to modify user pages by script.

The changes made were relatively harmless, but only because the author of the worm chose them to be. The Samy worm highlights the power of XSS, especially when it can be exploited en masse on traffic heavy sites.

How to Fix It

HttpOnly Cookies

Protecting cookies makes sure that information your site stores on visiting systems stays private and can't be exploited to pose as the original visitor. HttpOnly cookies restrict access to cookies so that client side scripts and cross-site scripting flaws can't take advantage of stored cookies. This should be enabled so that browsers that support HttpOnly can have the additional protection. Users with browsers that don't support HttpOnly cookies will still receive traditional cookies.

Vendor Recommendations

If a site is not using HttpOnly cookies, cookies should be destroyed after each use. This is a simple matter for all modern browsers, and a minor process step that can save a lot of trouble in the long run by never allowing authentication tokens to be misused. Additionally, using a private mode in the browser can prevent cookies from persisting.

Phishing Attacks and Fraudulent Email

Phishing attacks use email to impersonate someone, usually an authority figure, to try and trick an employee into transferring funds or disclosing sensitive information.

These attacks are much more likely to succeed when an organization doesn't take measures to verify and sort email before it reaches an inbox.

Problems UpGuard Detects

- SPF not enabled
- DMARC not enabled

In the Real World

The 2017 Verizon Data Breach Investigation Report (DBIR) revealed that nearly two thirds of all malware that led to breach or incident was delivered through email. Malware is responsible for more than half of all data breaches, so preventing email from being a malware inroad is crucial.
The infamous DNC hack, where Hillary Clinton's emails and those of her staff were leaked during the 2016 elections, came about as a result of a spearphishing attack on John Podesta, chairman of Clinton's 2016 campaign. Podesta was sent a fraudulent email claiming to be from Google that tricked him into handing his credentials over to probable IRussian hackers.

How to Fix It

Sender Policy Framework (SPF)

SPF works by publishing a simple TXT record in DNS, showing which servers are allowed to send email from that domain.

SPF Workflow

1. An SPF enabled email server receives an email from hello@upguard.com
2. The email server looks up upguard.com and reads the SPF TXT record in DNS.
3. If the originating server of the email matches one of the allowed servers in the SPF record, the message is accepted.

SPF should be enabled on all edge email systems to ensure that emails entering your organization can be checked for SPF, and that emails coming from your organization can't be impersonated by someone using an email server not listed in the SPF record. Failure to use SPF means your emails can't be checked for an authentic origination server and are therefore far less trustworthy than those that can.

DomainKeys Identified Mail (DKIM)
Unlike SPF, which applies on a per-domain basis, DomainKeys Identified Mail (DKIM) adds an encrypted signature on every message that can be validated by a remote server against a DNS TXT record. Essentially, organizations claim responsibility for email messages with their DKIM signature. Because signatures are encrypted, they are very difficult to forge; therefore an organization's reputation is on the line for messages sent out under their DKIM signature. DKIM signatures will be ignored by mail servers that do not support it, so there's no worrying about whether all your recipients are DKIM compatible. Failure to use DKIM reduces the integrity of your email and increases the likelihood of your domain being blacklisted.

Domain-based Message Authentication, Reporting and Conformance (DMARC)
The Domain-based Message Authentication, Reporting and Conformance (DMARC) protocol builds on SPF and DKIM to handle verification of sender domains. DMARC also provides reporting to give organizations visibility into their email policy. Additionally, DMARC specifies what to do with a message if the SPF and DKIM authentication mechanisms fail. The combination of SPF, DKIM and DMARC creates a trustworthy email environment. Failure to use DMARC means that SPF and DKIM policies will be different depending on where the message is sent. DMARC standardizes that by including instructions within the email itself.

Vendor Recommendations

When a vendor fails to have protection against phishing emails, all employees should be put on guard for emails from that company. Without SPF, DKIM, and DMARC, an attacker can spoof an email to make it look like it was sent from the vendor. Education about phishing in general and especially from the vendor's domain will help keep people vigilant with unsecured vendors.

DNS Hijacking

DNS is the mechanism that translates human-readable addresses like www.upguard.com into computer-readable IP addresses like 10.10.102.45. The problem is that DNS can be hijacked, and the human address can be pointed to a fraudulent IP address, with a dummy website set up, which gathers credentials and other information from people who go there.

Problems UpGuard Detects

- DNSSEC not enabled

In the Real World

In October of 2016, attackers hijacked a Brazillian bank's entire digital footprint by redirecting their DNS traffic to malicious sites. These sites used SSL encryption, and as such appeared with the padlock in browsers when people went to them, showing the clear need for Extended Validation (EV) certificates that can't be imitated. These redirected sites distributed malware to and phished personal information from visitors during the hijack.

How to Fix It

DNSSEC

There are several ways to exploit DNS, but DNSSEC prevents these by signing the DNS response using public key cryptography. This means that only authenticated DNS responses will be returned. When considering SPF, DKIM and DMARC, it should be clear how protecting DNS records is essential to email security as well— if the TXT records for these services are spoofed, it completely undermines the security they provide.

Vendor Recommendations

DNSSEC is a mechanism specifically designed to prevent this type of attack; however, it's use is not as widespread as it should be. Vendors who don't use DNSSEC are at a greater risk for DNS hijacking. Most businesses use what are called Extended Validation (EV) certificates for their websites. EV certificates don't just encrypt traffic, they validate the website owner, and can't be spoofed by malicious redirects. EV certificates display a green bar and the name of the company in the browser, so it's easy to double check that a vendor's site is legit.

Domain Hijacking

Internet domains, such as upguard.com, must be regularly renewed to function. The cadence depends on the hosting provider, but it's often enough that domain hijacking is a real problem. If a business fails to renew their domain before it expires, a malicious actor can pick it up as soon as it's available and host a fraudulent page, tricking people who think they are still going to the authentic domain.

Problems UpGuard Detects

- Domain expiring soon

In the Real World

If you think domain renewal only affects small companies, think again. In 2015, someone was able to buy the Google.com domain for $12. Fortunately in this case, the person wasn't out for money or malicious activity, and Google was able to reclaim the domain, with the domain purchaser giving the proceeds from this sale to a charity. However, few actors undertaking such a feat would be so altruistic, and even major domains need to be protected from hijacking.

How to Fix It

Internet domains are designed to expire after a specified interval. The key to protecting business domains is to create a trustworthy renewal process that monitors owned domains for expiry, catches them when they are close to expiration, and promptly renews them with the appropriate hosting platform. UpGuard monitors domain expiry for unlimited domains. This is rarely a concern for primary domains, which are watched much more carefully than other domains purchased and maintained by the organization, which may fall through the cracks. These ancillary websites are still a prominent risk vector, however, because any website that was once official can be spoofed to trick people who believe it still is.

Vendor Recommendations

UpGuard detects when a domain is about to expire, so organizations can be on alert, and complete their renewals in a timely fashion. Communicating this to the vendor can get them to renew it, or at the very least inform you of their process for doing so. If one of your vendors faces imminent expiration on their domain, employees should take caution around using services related to that domain around the expiration date, until proper renewal can be verified.

Reputation for Malicious Activity

Blacklists and other mechanisms for quarantining dangerous sites help protect organizations against sites that have a reputation for malicious activity.

Problems UpGuard Detects

- Suspected malware provider
- Suspected phishing page
- Suspected of unwanted software

In the Real World

These blacklists are the real world. Organizations on this list are or have been actively making the internet unsafe in real life. The reason these lists exist at all is to try and prevent people from being scammed or attacked by known sources. A false positive, or cleaning up after being blacklisted, can be time consuming and frustrating, but without these lists, everyone would be much more at risk for every type of internet attack.

How to Fix It

Suspected Malware Provider

If your websites show up on this list, it means that at one time they were detected serving malware to the internet at large. Since this is hopefully not by design, it means one or more perimeter assets was compromised and used maliciously for this purpose. The first step to fixing this is to audit and remediate all edge servers and network devices to ensure the malware is no longer present. Once this has been completed, you can petition the managers of the blacklist, such as Google, to remove your sites from it.

Suspected Phishing Page

If your domains are suspected for phishing attacks, it means that at some point phishing emails and other spam has been sent from your mail servers to the internet. Like malware, the first step is to ensure that this is no longer happening. Check mail logs to determine whether spam is still being generated. If so, take steps to prevent those accounts from sending email, disable them, and change the passwords. If not, or once you have stopped the malicious email, be sure to enable SPF, DKIM, and DMARC for your email servers. This helps prevent phishing emails and also increases email reputation, making it more difficult to end up on a phishing blacklist. Once these practices are in place, you can petition the managers of the list to remove your domains.

Suspected of Unwanted Software

Unwanted software is much like malware, except it comes packaged with advertised software. Often called spyware, these applications are silently installed along with a primary program, and perform malicious activity on any infected computers. If you are advertising software downloads from your website, check all downloadable files for bundled malware. Once all offered software has been checked and/or cleaned, you can petition the list for removal.

Vendor Recommendations

If your vendor shows up on these lists, that's a major problem. It means that traffic from their webspace has been shown in the past to be malicious. Asking the vendor why they are on it and what they are doing to fix it can help offer perspective, but doing digital business with providers on these lists carries a very high risk.

Dangerous Ports Exposed

Every digital service runs on a specific port. There are some ports, like 80 and 443, that are usually open to the internet. However, there are many more ports that should not be exposed to the internet at all, because doing so poses a major security risk. While some ports, like those for mail services, may be open by design, others, like database ports, should never be publicly accessible.

Problems UpGuard Detects

- Remote Administration
- User Authentication
- Database, Mail, VOIP
- Ransomware Susceptibility

In the Real World

The two major ransomware strikes that hit the world in 2017, WannaCry and Petya, both relied on a leaked exploit developed by the NSA called EternalBlue. This sounds high tech, but in fact it requires systems to have an internet-exposed Microsoft SMB port, a known security risk for some 20 years. There are a small number of scenarios where an internet facing SMB port might be needed, but in the vast majority of cases it is simply an oversight that leads to this extremely dangerous vulnerability.

How to Fix It

Open Ports

Just because a dangerous port is exposed, doesn't mean it shouldn't be, but it does mean that extra caution should be taken with services and assets running those open ports to the internet. If you discover open ports within your organization, the first thing to do is understand whether they are open by design for business functionality, or if they are open in error and can be immediately closed. For those that can't be immediately closed, compensating controls must be established around the services and servers hosting those ports to protect them from exploitation.

Some of these include:

- Enforcing strong password requirements, history, and regular changes on accounts
- Ensuring hardened configuration by regularly testing assets against benchmarks
- Isolate systems as much as possible and restrict service access to limit scope of exploit
- Monitor traffic on these ports and receive alerts for anomalies and irregular patterns
- Keep application software and all supporting software up to date and patched
- Consider using a VPN to access critical services instead of the internet

Vendor Recommendations

Many of the largest and most damaging cyber attacks only affect those systems with dangerous ports open to the internet. If your vendor has dangerous ports open, the data they handle for you might be at risk. If possible, limit datasets to anonymous and non-sensitive information. The risk of internet-facing ports can be mitigated through careful configuration, but they should raise a red flag that extra caution is needed.

Low Company Satisfaction

Business factors play into vendor risk as much as technical. Operations and processes are where vulnerabilities manifest. Unhappy employees, and negative company culture affect the way operations are carried out. Additionally, the more dangerous risk of an insider attack is much higher at an organization with low satisfaction and a distrust of company leadership.

Problems UpGuard Detects

- Low employee satisfaction
- Low CEO approval

In the Real World

Insider threats account for a significant portion of cyber attacks. Insiders are given access, and expected to act according to company policy with that access. When they don't, it becomes an insider incident. These incidents span everything from whistleblowers revealing information to the public, as in the case of Edward Snowden, to acts of revenge against a former or current employer, such as Ricky Joe Mitchell, who reset his company EnerVest's systems to factory settings, disrupting business for over a month.

How to Fix It

Low employee satisfaction and low CEO approval can result from a large combination of factors, almost all of them non-technical. Changing your corporate culture is outside the scope of this guide, but if your organization suffers in this area, some introspection is needed on behalf of leadership to try and turn things around.

Low scores in this area not only increase the risk of an insider attack or misuse of sensitive data, it also means operations are probably not functioning properly, which in turn leads to insecure assets and data. Most importantly, it means the business itself is at risk, and areas outside of cyber will also be more vulnerable. Establishing a transparent feedback mechanism, and making actual strides to improve based on feedback can course correct a failing culture if undertaken seriously by top level leadership.

Vendor Recommendations

There's not much you can do about another company's culture. But if your vendor has low ratings in this area, you can be on your guard about how you interact with them. Like with most cases, limiting access to systems and sensitive data greatly reduces the risk a vendor poses. Both operational oversight and insider misuse rely on valuable data or access. Practicing the principle of least privilege with your vendors is the best way to protect yourself.

High Organizational Risk

UpGuard scores organizations from 0-950. Those with scores below 600 are considered risky. In general, there are some best practices that can be followed to improve overall security and how to work with risky vendors to help protect your organization and customers.

Problems UpGuard Detects

- Organizations have a score below 600

In the Real World

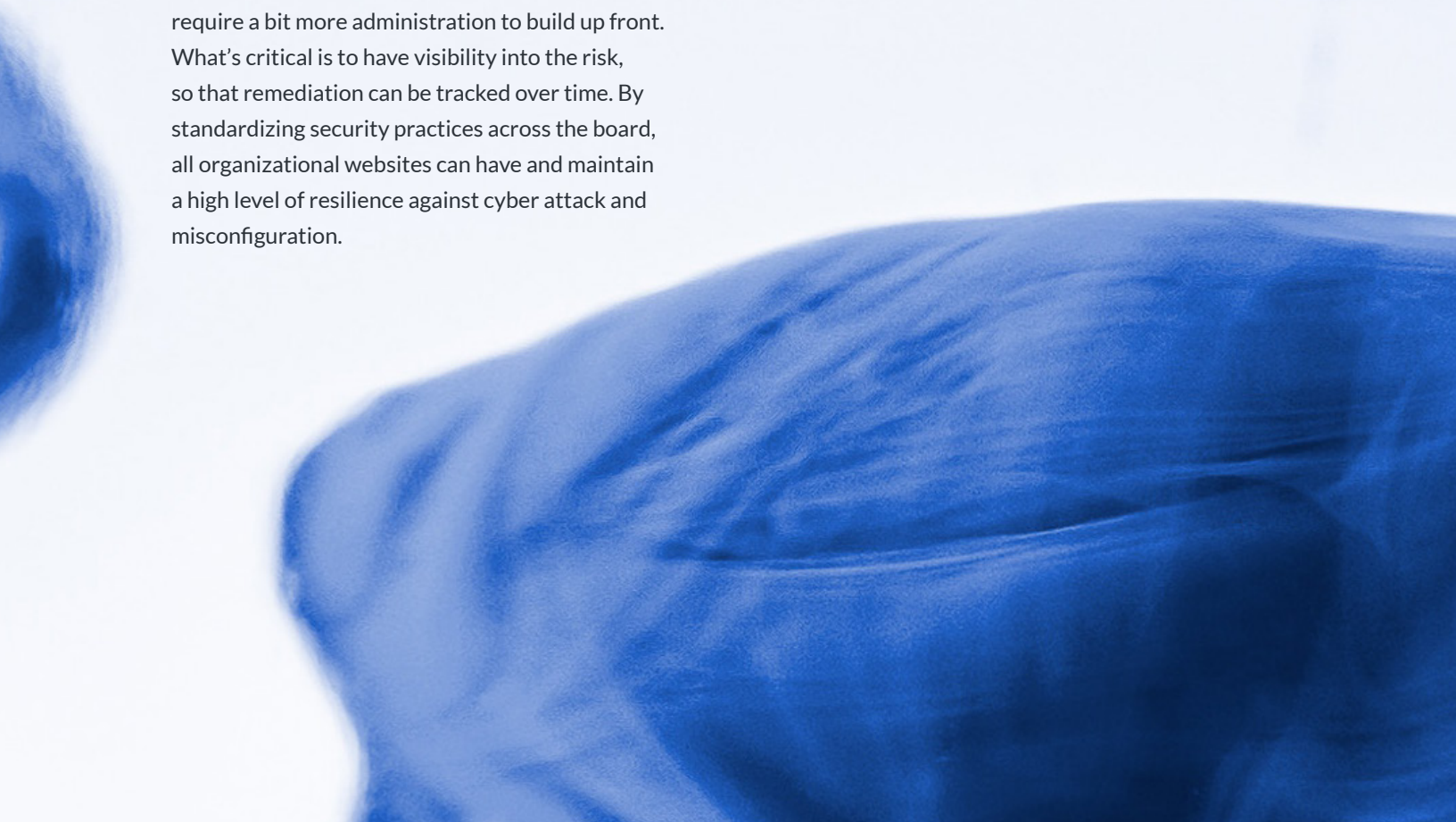
UpGuard has been leading the way in discovering cloud leaks and other misconfigured data exposures. We have found a clear correlation between having a low CSTAR score and likelihood of data breach. This makes sense, because CSTAR is based on the real risk factors for a breach, so those who score low have not shored up their defenses or secured their data handling processes, making it much more likely for a dangerous misconfiguration to enter production.

How to Fix It

If your websites generally have low scores, there are steps you can take to remediate them. The first thing to do is to have a clear and up-to-date inventory of all organizational websites, along with what threats they are vulnerable to. Once you have an established baseline and understand the security concerns, you can being to prioritize critical fixes in order of feasibility. For example, some threats can be mitigated by changing a simple directive within a config file. Others require building and propagating DNS records. Some, like DNSSEC, require a bit more administration to build up front. What's critical is to have visibility into the risk, so that remediation can be tracked over time. By standardizing security practices across the board, all organizational websites can have and maintain a high level of resilience against cyber attack and misconfiguration.

Vendor Recommendations

The number one thing you can do to reduce risk when working with an insecure vendor is to limit their access as much as possible. Following the principle of least privilege, they should be able to use only those resources which they absolutely need to perform their function. If they handle data, they should be given the minimal subset of data necessary. This at the very least limits the scope of a potential breach. Furthermore, employees can be warned that this vendor has substandard cybersecurity, and that communications from them, services on their website, and documents received should be treated cautiously, and not implicitly trusted. Usernames and passwords to services with these vendors should be unique, and not reusable within your organization.



Businesses depend on trust, but breaches and outages erode that trust. UpGuard is the world's first cyber resilience platform, designed to proactively assess and manage the business risks posed by technology.

UpGuard gathers complete information across every digital surface, stores it in a single, searchable repository, and provides continuous validation and insightful visualizations so companies can make informed decisions.

909 San Rafael Ave.
Mountain View, CA 94043
+1 888 882 3223
www.UpGuard.com