Startups & Data Breaches: How a Startup Can Protect Itself From a Data Breach in 2014 & Beyond

Thursday November 20, 2014

27 Data Security Experts Share The #1 Most Cost Effective Way a Startup Can Protect Itself From a Data Breach

As any business attempts to grow in today's technology-driven world, one of the top issues that any CEO or business manager must confront and continue to proactively address is data security.

For established companies, addressing the issue of data security can be made easier by enlisting the help of an established IT security vendor or by contracting an experienced data security expert. But for cash-strapped start-up companies, that isn't always an option.

Being in the data protection business, we set out to learn about data breach protection strategy specifically for start-up and early stage companies. We specifically wanted to discover expert tips from data security experts on what

meaningful, yet cost-effective way. To do this, we asked 27 data security experts to answer this question:

"What's the single most cost effective way a start-up company to protect itself from a data breach? "

We've collected and compiled their expert advice into this comprehensive guide on data breach prevention for start-ups. See what our experts said below:

Meet Our Panel of Data Security Experts:

- Ann Fellman
- Greg Sullivan
- Eric Basu
- Hassan Abdul-Zahir
- Brad Deflin
- Simon Gamble
- Michael Talve
- Anant Mendiratta

RELATED ARTICLES

The Evolving Managed Security Model
By Mike Pittenger

Hybrid Managed Services Offer the Best of Both Worlds for Security Deployments

- Bryant Tow
- Stu Sjouwerman
- Istvan Lam
- Dennis Turpitka
- Jennifer Searfoss
- Aaron Messing
- Raees Mohamed
- Neal O'Farrell
- Keith Alexander Ashe
- Kevin Coy
- Max Dufour
- Arthur Zilberman
- Sam Cornish
- Justin Farmer
- Ted Devine
- Gene Shablygin
- Chris Kirby
- Rich Silva
- Uzair Gadit

Arthur Zilberman

@laptopmd

Arthur Zilberman is the Founder and CEO of LaptopMD.com, a full-service computer repair company specializing in computer repair, data recovery, and other IT services. Born in Minsk Belarus, he emigrated to Sheepshead Bay as a child and graduated from NY institute of Technology with a BS in computer science. Before LaptopMD, he primarily worked as a corporate IT manager for fortune 500 companies such as JPMorgan Chase.

As the owner of an IT service, what I've learned is the key to protecting data as a start-up or otherwise lies with...

How you store it.

To reduce liability and potential infiltration/data theft, the best practice is to store your data locally. Try not to store sensitive information (IE customers' financial information) on servers. If you must utilize a web hosting service, make sure they use the most up to date encryption and they consistently communicate with you. A good hosting service will inform a small business of a potential vulnerability whereas smaller companies may leave you in the dark. That could be the difference between information protected and information stolen.

Along with minding where information is stored, small business owners should run consistent antivirus scans and put up firewalls to ensure there are minimal chances for data to be reached by any outside sources.

Ann Fellman

@code42

Ann Fellman is the Director of Product Marketing at Code42, an endpoint data management company.

When it comes to the single most cost effective way a start-up company to protect itself from a data breach, this is

It's lonely in the middle -- but it doesn't have to be
By Dan Geer

For the middle class of companies, information protection is especially hard.

Left of Boom: The Importance of Protecting Critical Data
By Paul Roberts, Editor, The Security Ledger

Identifying your 'crown jewels' is a key step in modern risk management. It's also much easier said than done.

effective way a start-up company to protect itself from a data breach, this is my advice...

No matter your size business, it's imperative that IT maintain visibility over what your employees are doing with your company data, and which tools they're using to store, sync and share it.

We're in an age where the line between personal and business devices is blurred, and with a mobile workforce, it's difficult to keep track of where your business-critical data ends up. Unfortunately, consumer cloud file sync/share tools introduce the risk for data breaches—and most often employees unknowingly introduce risk to your organization by simply syncing data across their devices or when working with others outside the organization.

At a minimum, your company should establish data security policies that include guidelines for file sharing. While consumer sync/share tools may be widespread among your users for personal sharing, organizations need to carefully vet the security and encryption practices when it comes to sharing business data. Organizations need a clear understanding of where data is stored, if it's encrypted and ultimately, who has the keys to the data. That's why we built SharePlan— enterprise-grade, secure file sync and share deployed on-premises behind a company's firewall. It's built with a security-first mindset so companies can offer employees sync/share knowing they're meeting even the strictest data security and compliance obligations. And employees readily transition away from consumer cloud tools because of SharePlan's smart, easy user experience.

Greg Sullivan

Greg Sullivan is CEO for Global Velocity, a company pioneering new approaches in securing information. Mr. Sullivan is recognized as an industry expert and visionary in the field of cybersecurity. He is the retired Founder & CEO of G. A. Sullivan, which Greg formed in 1982 and built into a leading software development company. Ernst & Young named Sullivan a 2000 Entrepreneur of the Year in the software/information services category and the U.S. Small Business Administration named Sullivan the 1999 National Small Business Person of the Year.

The most cost-effective step a start-up can take to preventing a data breach is...

To realize that the traditional approach of relying on antivirus, firewall and anti-spam software tools is growing less and less effective.

Symantec's recent admission to the Wall Street Journal that antivirus software is "dead" is a big red flag that this approach of hardening the network and data stores is insufficient, particularly as companies increasingly move their data to cloud-based services. Smaller businesses are the top adopters of cloud computing services. The priority must shift from protecting information from the outside-in to securing it from the inside-out, an approach I call "information-centric security."

While SMBs are not as big as companies like Target and Home Depot, they are the majority of victims at the hands of cyber thieves seeking easy targets. The Verizon 2013 Data Breach Investigations Report found that 62 percent of breaches impacted smaller organizations, likely a conservative figure since not all small organizations are reporting breaches.

The issue is that SMBs wrongly assume that their size or small influence does not merit attention from hackers or do not educate themselves about potential exploits in their infrastructure. Hackers run their operations like a business and want to find ways to maximize the return on their investments. That makes small businesses, which typically do not have the IT resources or expertise to implement and manage security systems, prime targets. A Ponemon Institute survey reported that one-third of respondents admit they are not certain if a cyber-attack occurred in the past year, and 59 percent of SMBs say they do not have sufficient IT experience.

Instead of securing data from the outside-in, organizations must adopt an information-centric approach. This requires monitoring where files are kept, how they are used and where they are being sent to in order to prevent a breach. There is still value to hardening your network and using endpoint security software to try to keep the bad guys out, but those steps are now part of a larger strategy that must address the fact so much information is outside the company's servers and being accessed by so many different devices.

You must know exactly where sensitive data lives at rest, employing technologies like document fingerprinting, pattern matching, keyword dictionary comparisons and other techniques that can track the genealogy and chain of custody of digital files.

You should also be aware of how your sensitive data is being used in motion, and that requires pervasive monitoring to identify meaningful deviations from normal behavior that signal malicious intent. This can include examining file location, the time of day, what devices are being used, IP addresses and URL reputation.

This combination of content aware monitoring plus context aware monitoring equals information-centric security: knowing your digital assets are protected against unauthorized use, disclosure, modification, recording or destruction.

A number of vendors, including mine, offer cloud-based solutions that do not require the startup or small business to install and manage software on-site. Everything is automated and accessible through a management console, and rules for how suspicious activities are treated, and how the companies are alerted, are set by the individual company.

Traditional antivirus software is not obsolete, but the practice of solely relying on it to protect your data is. It simply cannot keep the bad guys out, and when those attackers do break through the network security system, they can sit quietly for months or even years stealing data before they're discovered and the damage is done. The fact organizations are moving more information to cloud or SaaS-based services, and permitting employees to access that information with their own personal devices, makes an attacker's job easier and increases the risk of accidental loss by a well-meaning employee. Adopt an information-centric approach that enables real-time monitoring of data at-rest and in motion to better protect what the cyber thieves value the most - your data.

Eric Basu

@SentekGlobal

Eric Basu, past finalist for Entrepreneur Magazine's Entrepreneur of the Year Award, is the Founder and CEO of Sentek Global, a Inc. 5,000 company focused on developing cybersecurity and information assurance programs for a wide range of corporate and government clients. He is a former U.S. Navy SEAL who fosters this warrior engineering and esprit de corps values system to both his company and valued customers.

It's not getting the most up-to-date anti-virus, anti-spam or highly-rated firewall. It's far more rudimentary than that. The single greatest thing any company can do to protect itself from a data breach is...

To spend a fraction of those dollars on training their team to avoid doing simple things that leave themselves vulnerable to cyber attacks.

Most start ups will operate in a virtual environment where their employees are often scattered across different zip codes and time zones. Taking the time to train team members on prudent cyber practices is essential. These may include, but aren't necessarily limited to utilizing only trusted WiFi networks, never leaving devices outside of one's control, utilizing good password practice and such. The most vulnerable access points to a company's networks are often the unintended consequences of an employee's day-to-day practices. Training team members on the do's and don't can go a very long way into protecting sensitive data.

Bryant Tow

Bryant Tow is the Chief Security Officer for Vaco Risk Solutions in Memphis, Tenn. Bryant supports the Vaco Risk Solutions team by contributing to strategic direction, solutions development and sales support. He also serves as Vice President of the FBI's InfraGard National Members Alliance, is recognized as a Distinguished Fellow at the Ponemon Institute and has published several books and articles on cyber security topics.

When it comes to the most cost effective way a start-up can protect itself from a data breach, here is my advice...

A start-up must first realize that it is under attack.

Small businesses are by far the largest attack surfaces for cyber criminals because most do not pay attention to security, don't allocate any budget to security and have few to no resources.

A company should identify the critical assets of the business.

As companies get started there may be a perception that there is nothing to

protect. Every business must have something that makes them unique in the market place, and which also makes them a prime target for cyber criminals. Take the time to understand where the value is within the business and give it the proper protections.

Finally, a start-up should consider outsourcing.

On average, big businesses see cyber-attacks numbering into the billions per day. There is no way a startup company can keep up with the threat. Until such time as it is financially viable to house internal threat intelligence, it makes sense (and cents) to leverage an organization that gives you the same vision and analytics as your larger competitors.

Stu Sjouwerman

@StuAllard

Stu Sjouwerman is the Founder and CEO of KnowBe4, LLC, an IT security company, and an IT Security expert with 30+ years in the industry. Sjouwerman (pronounced shower-man) was also the Co-Founder of Inc. 500 company Sunbelt Software.

The single most effective way to protect yourself from a data breach is...

Security awareness training. Its cheap and for the very small - it is free.

The vast majority of data breaches come from human error and social engineering. Ransomware is one of the top ways and can affect any size company. Here are some specific security tips I would advise:

1. Don't click on anything suspicious or any type of attachment you are not expecting.
2. Hover over a link to make sure it is a valid link.
3. Back up your data. Use multiple forms of backup as backup often fails. Test the restore function and make sure it works.
4. Train your staff on security awareness training.
5. Don't pick up any stray USBs and don't plug them in!
6. Use a password tool like LastPass to protect your passwords.

And remember - think before you click!

Istvan Lam

@Tresorit

Istvan Lam is the Founder and CEO of Tresorit, a secure cloud storage solution that utilizes zero knowledge end-to-end encryption, and the co-inventor of Tresorit's encryption technology. Prior to founding Tresorit, Istvan served as a student researcher at the Ecole Polytechnique Federale De Lausanne in Switzerland and a student teacher at the Budapest University of Technology and Economics. In addition, Istvan has spearheaded

Challenge24, a 24-hour long programming contest held annually in Budapest.

A simple and easy solution that won't break the bank for start-ups is...

To store their data on a cloud solution that incorporates data-centric security as opposed to application-level security, meaning that security measures are embedded in the data itself as opposed to focusing all protective measures on infrastructure.

In the scenario of a data breach, and if documents are enabled with data-centric security, access to those files can be revoked remotely.

Dennis Turpitka

@Apriorit

Dennis Turpitka is the Founder, CEO, and General Manager of Apriorit, a software R&D company founded in 2002. Besides cooperating with a number of leading vendors around innovative R&D projects, Apriorit also founded several security technology spin-offs namely Hypertection, Cloudifile, and Ekran System.

The most cost effective way for a start-up company to protect itself from a data breach is…

Continuous monitoring - with a "simple security" approach.

The basic and traditional answer is continuous monitoring of work with security data with suspicious and potentially harmful actions alerted ASAP. There are a huge number of [privileged] user activity monitoring solutions on the market now, but the most of them are not really suitable for a start-up, as they usually require a pro security expert to work with them.

For a start-up with limited staff extremely focused on R&D and biz dev, hiring such an expert is a luxury. So I think, it's about the monitoring process/results format. Is should be integral, easy to understand and quick to analyze requiring minimal non-specific technical skills. Keyword-indexed session video records can be an option, if additionally supplied with easy episode search, alerts, and simple analysis tools.

Jennifer Searfoss

@SCGhealth

Jennifer Searfoss, J.D., C.M.P.E. is the CEO of SCG Health. SCG Health opened in 2011 and is focused on revenue cycle management and strategic planning in this post-health reform world. Services support the business of medical practice including physicians, medical groups, software companies and associations.

The most cost effective way a start-up company can protect itself from a data breach is...

Encryption. Encryption. Encryption.

Without it, your health care related activities are considered a breach. And it makes your company less attractive than someone else's. That is really the goal! Look for a solution that is double authenticated for the user and stores the encryption keys on a different server than the secured message or data. After encryption, look for a secure server solution which is not the big server farms. Check out the new small business solutions from Microsoft and Google. They are reasonably priced and offer the backing of big companies who have figured out how to do this reasonably well.

Aaron Messing

@amess

Aaron Messing, Esq., CIPP is an Attorney at OlenderFeldman LLP, a law firm providing customized financial, technology, intellectual property, information privacy & data security, startup company and litigation services. He has been been quoted by a number of leading media publications including the New York Times, Business Insider, U.S. News and World Report, Fox Business News, CIO.com, Techworld, Computerworld, and others regarding startups, cyber security, data privacy and other legal issues. Aaron also serves as Chief Privacy Officer of Advanced Health Media LLC.

The most cost-effective way for startups to protect themselves from a data breach is by...

Encrypting sensitive information. Even if encrypted information is breached, it will be unusable, and encryption technology is relatively cheap.

Hassan Abdul-Zahir

Hassan Abdul-Zahir is Co-Founder and Chief Technical Officer of North Coast Security Group (NCSG). He has worked in technology and security over the last ten years in large retail and healthcare organizations. His primary role is to oversee the development of the hardware and software platforms ensuring co-operability and synergy between the two.

For a startup company that already has to manage all of the other costs associated with a new endeavor, finding a cost effective solution while maintaining the highest level of data protection is as important as it’s ever been. The single best security solution for a startup is...

To invest in a Unified Threat Management (UTM) device.

A UTM device combines the features of multiple devices in one; think of it as the equivalent of purchasing a printer/copier/scanner/fax all in one instead of

buying all of these as separate devices. A UTM device can be deployed in variety of variations, such as a firewall, a proxy server, a web content filter, and a VPN gateway just to name a few. A UTM device can protect both the local network and remote users simultaneously providing a high level of protection for all team members of the company.

Brad Deflin

@BradDeflinTDS

Brad Deflin is President and Founder of Total Digital Security (TDS), an information systems security solutions provider that specializes in mitigating and managing online risks for families, professionals and small businesses.

The most cost effective way a start-up can protect itself from a data breach is by...

Staying away from hardware as much as possible.

Today, you don't need large upfront costs and IT expenses to protect your data and digital assets. Effective cyber-security is a service, not a product, and can now be managed and administrated by software and the internet. Powerful, cloud-enabled "managed security as a service" solutions are available for a very low monthly cost, usually less than $100. The services are effective enough to achieve compliance with even the most rigorous of digital security requirements, such as PCI and HIPAA.

Raees Mohamed

@KellyWarnerLaw

Raees Mohamed, Esq. is Corporate Lawyer at Kelly / Warner, PLLC who advises startups and entrepreneurs on the best data and privacy practices. Raees focuses on advising SaaS clients and web-based businesses. He is also an Adjunct Professor of Law at the Sandra Day O'Connor College of Law at Arizona State University.

"You can't be serious?" That's the reaction you're going to get when your founder learns that a data breach occurred. So what's the single most cost-effective way that your startup can prevent one? The answer is...

To create and enforce effective data and privacy practices.

While cloud-based security solutions, security hardware, and encryption are all important, those tools get you nowhere if you are not implementing them correctly. Effective data and privacy practices must start from the top-down, with founders creating written agreements between themselves, and with vendors and customers, and internally through policies among employees and contractors. As a tech start-up, your most likely source of breach will be...you guessed it, an internal mishap by an employee or contractor, not a hacker.

Your startup's policies should state: what is considered "data"; how to manage data; how data can be accessed; who can access it and when; what's considered a breach; a to-do list when a breach occurs; all of which should be strictly enforced with no exceptions. Legal mandates in your industry should dictate how to fill in these elements of your policies (think COPPA, HIPAA, FERPA, CIPA, etc.). Let's face it, you can have the best security systems in place, but without clear written protocols, those systems offer zero value. You can't address data breach unless you know the most likely sources of breach, the liability exposure once a breach occurs, and have written policies to prevent them (and to address them if they occur).

Think of your data and privacy practices as your championship playbook. You can have the best players in the league, but if they don't know what to do, their talent is all in vain, and you'll lose the game. Besides, who would do business with a startup that doesn't care about their data?

Neal O'Farrell

@nealofarrell

Neal O'Farrell is the Security and Identity Theft Expert at Credit Sesame and is the nation's Number 1 Consumer Security Advocate and a nationally respected expert who has been fighting cybercrime and identity theft around the world for thirty years. He is regarded as one of the early pioneers of the cyber security industry and has developed advanced encryption systems to protect sensitive communications systems for governments, the military, and the financial industry. Neal is also the Founder and Executive Director of the Identity Theft Council, a national non profit dedicated to helping victims of ID theft. As Executive Director of the Identity Theft Council, Neal has personally counseled thousands of identity theft victims, taken on cases referred to him by the FBI and Secret Service, and interviewed some of the nation's most notorious identity thieves.

For established and startup companies alike, the single best way to avoid a data breach is...

To make sure everyone involved in the company - founders, employees, and contractors - lives and breathes security and privacy into every minute of their day. It won't just help avoid data breaches, it will send some very comforting signals to your customers.

It's not enough simply to focus on the obvious, like payment processing systems. Even a database of customer email addresses, for something as benign as a newsletter, can harm customers and company reputation if exposed.

Years ago I had a security startup, developing advanced and sensitive encryption for government and the intelligence community. Phone surveillance was a major problem and every phone in the office had a sticker that said 'Mind What You Say.' A not-so-subtle way to make sure that security awareness and vigilance were a top priority for everyone.

Keith Alexander Ashe

@keithashe

Keith Alexander Ashe is the CEO, Founder, and Lead Developer at Spendology LLC. Spendology is a technology company that creates content, software and services that activate financial intelligence.

Here are my top security tips for startups:

1. Secure: HTML inputs use the ' type="password" ' for text inputs tags to mask user passwords. For example: Text input would show user's password `<input *type="text" *name="password">` Text input would mask user's password `<input *type="password"* name="password">`
2. Encrypt data stored in databases. Learn more about encrypting data with server-side scripting languages on w3chools.com or stackOverflow.com.
3. Use SSL Certificates (Secure Socket Layers) to protect info as users submit it.

Kevin Coy

Kevin Coy is a Partner in Arnall Golden Gregory, LLP's Privacy and Consumer Regulatory Practice based in Washington DC. Mr. Coy advises organizations of all sizes on privacy and data security issues, including data breaches and breach mitigation.

No one step will protect start-ups, or established businesses for that matter, from a data breach. But one thing that would reduce the potential fallout from an incident is...

Encrypting as much personal information as possible (assuming the encryption keys were not also compromised).

Looking beyond encryption, another way in which a start-up can work to protect itself from a data breach is to collect only the minimum amount of information necessary for its business. In short, if it hasn't been collected then it can't be breached.

A start-up also should also be careful to protect any personal information that it collects, encryption is only one strategy in this regard. A start-up would be wise implement an information security program tailored to its business in order to protect any personal information that it holds or other parties collect or maintain on its behalf.

Do not forget about service providers. A start-up can be legally responsible for a breach of its information while it is being held by one of its service providers, just as if the information were being held in-house.

Max Dufour

@maxdufour

Max Dufour is a Founder of Harmeda, a Technology and Strategy firm. Max has been involved with many security assessments over the years as clients were building up or enhancing their technology set ups by transitioning to new solutions, to the cloud and to mobile platforms.

The most cost effective way for a start-up company to protect itself from a data breach is…

Penetration testing: the best tools and the best strategy need to be tested, especially if the firm is new and cannot afford yet all the bells and whistles, nor the time to build a holistic security set up.

The highest risk is for small firms with a lot of sensitive data, for example marketplaces, where a start-up would collect a lot of credit card data and pass it on to third parties to support transactions. Consultants and software solutions can certainly help address most data breach risks but you would still want to test attempts at accessing that data in a real fire scenario. Would the attempt get noticed right away? What would be the reaction to it?

The best time to go through this exercise is once all systems have been deployed and security systems are up and running but ideally before Go Live. Additionally, after each major upgrade or change in the product portfolio, it makes sense to test again, ideally using a different firm or approach to validate that the data is still secure when the company is attacked by hackers, malware or other means.

The major challenge with data security is not a lack of tools but instead an abundance of creativity on the market where many individuals are hard at work, seeking to cause irreparable damages from a safe distance. Startups need to pro-actively tackle security before they get impacted by a breach and a potential crisis which could impact their survival.

Sam Cornish

Sam Cornish is a Cybersecurity Expert with Genova Burns Giantomasi Webster, and a member of the firm's Complex Commercial Litigation and White Collar Criminal Defense, Corporate Internal Investigations & Corporate Ethics Practice Groups. Founded over twenty five years ago, Genova Burns Giantomasi Webster represents many of the premier companies and business interests throughout New York, New Jersey and Pennsylvania. He has guided corporate officials whose companies have had data breaches through the minefield of agency reporting requirements and public scrutiny, and has written cybersecurity policy manuals and led investigations into the causes of a breach.

The most cost-effective way for startups and small businesses to reduce risk is...

Minimizing the amount of protected information in their possession.

Startups should not collect protected information from customers and employees unless they truly need it for operations. Along the same lines, protected information should only be maintained as long as necessary and then destroyed.

An equally crucial, but often overlooked concern is the cyber vulnerability of a business's vendors.

Earlier this month, Dairy Queen announced that approximately 400 of its locations may have been affected by point-of-sale malware that hackers use to collect consumers' credit card information. They got in, Dairy Queen said, through a compromised third-party vendor account.

Target's data breach in 2013 similarly resulted from a vendor-based vulnerability.

To reduce the risk of a data breach or other exposure of protected information, businesses need to have vendor risk management policies and processes in place that include:

- due diligence and risk assessment prior to vendor selection;
- well-crafted written agreements with security requirements and post-incident response obligations clearly defined;
- narrowly-tailored administrative privileges and access rights; and
- ongoing monitoring of vendors, including periodic reassessments.

Not only is vendor risk management prudent, but many U.S. businesses have such obligations under federal or state law. That's particularly true for healthcare providers, financial institutions and in Massachussetts, businesses that maintain personal information about that state's residents.

The law, for many businesses, and prudence, for all businesses, dictate the implementation of risk management for vendors that handle or have access to a business' sensitive or protected information. Other measures exist, such as including liquidated damages clauses, indemnification obligations, and insurance requirements in agreements with vendors.

But vigilance is the key, as breaches are more likely to be caused by human error than by a successful cyber-attack.

Simon Gamble

@MakoNetworks

Simon Gamble is President of Mako Networks North America, a company that specializes in assisting small businesses to build simple, secure cloud-managed networks. He has more than 15 years of experience in secure networking, first establishing the company in New Zealand and now managing its international growth in the United States.

A secure business starts with having secure network environment. It lays the groundwork for all other areas of the business - secure payments

processing, secure data storage, and secure devices in the workplace. And a secure network is smarter than the employees that use it - which is critically important, as people are generally regarded as being the weakest link in the chain. Small and startup businesses should start their search by...

Protecting their Internet connection with a strong firewall or network gateway, preferably one with independent certifications from recognized third parties, like ICSA Labs or the PCI Council.

These devices should also provide reporting functions to provide the startup with information on how their network is being used, so any potential security issues can be detected before they become full-scale data breach events. And if startups are processing payments as part of their service, then they need to take the time to become familiar with the Payment Card Industry Data Security Standard (PCI DSS) - a special set of requirements that govern how payment data must be secured within a business. The full PCI criteria consist of more than 200 technical and procedural requirements, so there is some degree of work to be done to ensure that a business meets its obligations. If they don't, they're at risk of significant financial penalties and lost business. Nearly 60 percent of small businesses that suffer a data breach are out of business six months later.

Michael Talve

@mtalve

Michael Talve is the Founder and Managing Director of The Expert Institute, a technology-driven platform for connecting qualified experts in every field with lawyers, investment firms, and journalists looking for technical expertise and guidance.

For a start-up with limited capital to spend on internal data security solutions, oftentimes the best solution may be...

To contract out data security by placing everything in the cloud.

By using Salesforce to manage the majority of our data, we are able to provide technical security without maintaining expensive internal systems for data management. The beauty of Salesforce is that it can neatly scale with our growth without much hassle, since we can just expand our data usage with their platform.

Otherwise, we make sure to enforce best practices for data security on the human side of our business e.g. who can access what data, password protection, etc.

Anant Mendiratta

@anantmendiratta

Anant Mendiratta is an Entrepreneur and the Founder of WiseCalvin, a digital marketing firm. He is a digital marketing geek who learns,

coaches and works 24 x 7 to help startups and businesses succeed online.

The most cost effective and easy way for a startup to protect itself from a data breach would be...

To enforce strong passwords across your entire systems. To test the strength of your password, here's a tool you can use http://www.passwordmeter.com/.

Justin Farmer

@myneobot

Justin Farmer is the Co-Founder of Kernel, Inc. and inventor of Neo, a the simple to use security assessment appliance for businesses of all sizes. Justin has over 15 years of experience in the information security industry and provides data-security solutions for multi-national companies around the world in wartime areas.

An incredibly simple and cost effective solution for a start-up company to protect their data is...

To buy a firewall that sits between their business network and the Internet.

Simply installing the firewall isn't enough though, it takes a little bit of configuration which can be done by reading the manual that comes with the firewall and/or watching configuration tutorials that vendors and users put online.

If the start-up budget allows, it's also worth it create a simple security audit and update procedure. At this point, the procedures don't need to be overly complex. Instead, focus on making sure that your systems and installed software are always up-to-date through standard patching and update programs that come with the software and operating system. For instance, Microsoft patch Tuesday is the 2nd Tuesday of each month which means updates should be applied quickly after their release.

Still depending on the budget, there are affordable solutions to help protect your internal and external network from hackers as well. These tools provide the valuable service of vulnerability identification so you know the areas in which a hacker would probably attempt to use to gain access to your data. Many of these tools provide different levels of information for you to use to close security holes.

Ted Devine

@InsureTechBiz

Ted Devine is the the CEO of TechInsurance, the nation's leading online agent for IT freelancers, independent contractors, and small businesses.

When it comes to data breaches, one of the best things that startups can do is...

Invest in insurance - the only thing that can protect them when their data is hacked.

Data security experts will tell you that there is no sure-fire way to totally protect a business against data breaches. A determined hacker will get in. But the more important question for tech startups is: What happens after a breach, when a client alleges that the developer's code was not adequately secure?

If, for instance, software accesses or stores data for a client's customers, there's a huge loss exposure from a data breach. Think about it: the client has an embarrassing, possibly catastrophic, situation on their hands and will be required to formally notify all of their affected customers and, in some cases, provide credit monitoring to them.

Not only will the startup likely lose the client, but they may even be sued, along with every other outside contractor connected with the client's software and IT infrastructure. Fortunately, most Errors & Omissions policies for small IT businesses include coverage for this – it's called third-party Cyber Liability – and it protects against the cost of the lawyers and any damages or settlements for these types of cases. Most IT businesses are getting E&O anyway, so it's just a matter of talking to their agent and making sure the third-party Cyber rider is in that policy.

Gene Shablygin

@WWPass

Gene Shablygin is a nuclear physicist turned IT entrepreneur who is the Founder and CEO of WWPass, a data security software firm.

Without question, the most secure and affordable way for start-ups to prevent data breach is...

Two-factor authentication.

Far too many early-stage companies rely on traditional username and password combos or one-time passwords to allow employees to log on to secure networks, apps, web portals and more. Modern hackers are absolute experts at cracking those. They've succeeded at it for decades.

Two-factor provides a second layer of protection, usually in the form of a physical token like a USB device or a secure mobile app. Users have to provide not just something they know, like a password, but also something they have. Even if hackers get their hands on passwords, they still can't access sensitive data. Cybersecurity experts have long stressed that two-factor is a far better option, but many start-ups aren't aware of that. When it comes to choosing a vendor for two-factor, there are many options and not all are equally secure. But some form of two-factor is always better than none. Two-factor is also affordable: some of the most secure options cost just a few dollars a month or less per user.

Startups also need to pay careful attention to how their data is handled and stored, particularly when working with cloud vendors. They should be looking for vendors that encrypt and fragment the data to keep it out of the hands of hackers. They should also develop clear internal policies for how sensitive data is handled and stored. Can employees send information via mobile devices? What types of emails must be encrypted? How are employee laptops protected so that information can't be compromised if they are stolen? Sometimes a data breach is simply the result of an employee mistake, and good policies help prevent that -- for free.

Chris Kirby

@voicesdotcom

Chris Kirby is the innovative IT Manager at Voices.com, the industry-leading website that connects brands with professional voice talent. Voices.com has been written about in The New York Times, CNBC, CNNMoney, BusinessWeek, Forbes Magazine, Success Magazine, Entrepreneur Magazine, Fast Company, The Verge and The Wall Street Journal's Accelerators Blog.

The best and most cost-effective way a startup can deal with the possibility of a data breach is...

Being proactive.

Protect everything, secure everything, encrypt everything. Don’t wait for the breach to happen. Identify the bad guys early (when they are only probing) and lock them out of your infrastructure. Make sure that if they do get their hands on anything - it is useless to them.

Rich Silva

Rich Silva is the Founder and President of Pain Point IT Solutions Inc., a Managed IT Services Company headquartered in Poughkeepsie, New York. After a 19 1/2 year run as a manager of a Network Engineering group and IT Support group for the same company, Rich took the leap of faith and started his own company with the goal to provide small and medium sized businesses without full-time IT personnel the tools they need to maintain their IT and telephony systems.

Too many assume that data breaches are outside jobs originated from somewhere outside the company. While this much of this is true, these perpetrators look for someone unknowingly to "leave the key in the door" in order to enter the domain. The single most cost effective way a start-up company can protect themselves from a data breach is...

Through social engineering, learning best practices, and drafting acceptable use policies for accessing work computer systems. Then when the money

starts coming in and everyone is educated and aware that they're holding these proverbial keys, fortify the domain with a intrusion detection system.

Uzair Gadit

@purevpn

Uzair Gadit is a Serial Entrepreneur, Technology Specialist and the Founder and Director of PureVPN, a VPN service provider that operates a rapidly expanding self-managed VPN network with the most diverse range of security, privacy and anonymity solutions.

What's the single most cost effective way a start-up company can protect itself from a data breach? To answer this question, it is important to get delve into the major factor causing data breach especially for businesses...

The most important ones are Web based threats – Spam Links & Attachments, Weak Protocols to transfer data, Low data encryption, insecure access by employees.

What has been experienced through the business hacks occurred in the last couple of years is that the biggest and the easiest way to attack any business is through 'Insider Misuse', which is when an employee from local or international branch access the company's server/network through insecure mediums such as free WiFi hotspots or Public ISP etc.

Apart from that the weak encryption (Usually because of using free mediums) of data transfer between 2 or more locations give chances to the hackers to sneak through it which cause serious damage to the startups on their expansion and business confidentiality.

Comments

Please post your comments here

Your name *

As you would like it displayed

E-mail

The content of this field is kept private and will not be shown publicly.

Comment *

Math question *

3 + 3 =

Solve this simple math problem and enter the result. E.g. for 1+3, enter 4.

Submit