An Expert Guide to Securing Sensitive Data: 34 Experts Reveal the Biggest Mistakes Companies Make with Data Security

Wednesday October 8, 2014

Keeping sensitive information secure from theft and vulnerability in today's digital world isn't as easy as putting a lock on the file cabinet - especially with the widespread adoption of cloud computing. And even if you take every precaution with your online accounts and identifying information, there are many ways that information can land in another individual or company's data management systems, where it can then somehow be made vulnerable.

At Digital Guardian we specialize in helping businesses manage and secure various types of company data. Our top priority is helping our customers keep their sensitive data where it belongs and as secure as possible. To get a better picture of the current state of enterprise data protection we interviewed data security experts on what matters most when securing sensitive data.

To do this, we asked 34 data security experts to answer this question:

"What's the #1 biggest mistake companies make when it comes to securing sensitive data?"

We've collected and compiled their expert advice into this comprehensive guide to effectively securing your company's sensitive data. See what our experts said below.
Meet our Panel of Data Security Experts

- Michael Howard
- Paul Ferguson
- Jonathan Gossels
- Amit Pamecha
- Dr. Scott Nelson
- Jack Wilson
- Colin Lobley
- Michael Fimin
- Joe Moriarty
- David Arnoux
- Alan Baker
- Stelios Valavanis
- Eric Jeffery
- Jeremy Ames
- Steve Marsh
- Dave Oder
- Ivo Vachkov
- Andrew Bagrin
- David Mohajer
- John Dancu
- Christopher Stark
- HK Bain
- Amit Bareket
- Patrick Oliver Graf
- Chuck Davis
- Liam Fallen
- Paul Banco
- Drew Farnsworth
- Rich Reybok
- Aaron Ross
- Ryan Satterfield
- Kevin D. Murray
- Mark Nicholas
- Matthew Turner
Michael Howard

In the past year, 92% of Forbes Global 2000 companies reported data breaches with an average cost of $136 per record compromised and $5.4M overall. With an evolving technology landscape that is increasingly connected, maintaining a secure IT environment is more important now than ever before.

The most common pieces of technology that companies secure include PCs and network servers. However, the biggest mistake companies make when it comes to securing sensitive data is…

Not securing their printing fleet.

Nearly 90% of enterprise businesses have suffered at least one data loss through unsecured printing. Luckily, there are preventative steps that business owners and IT managers can take to ensure that their workplace doesn't experience the same security issues.

- **Audit your print environment**: Companies should consider conducting an audit of their print environment utilizing rigorous standards from the National Institute of Standards and Technology. This reduces network security risks and improves compliance without adding to IT overhead.

- **Install proper security software**: There are a variety of differentiated software solutions that can help secure your technology. Considering a risk monitoring solution could help companies identify and highlight potential risks, making it easier for IT to manage. This not only keeps data and devices secure, it also helps slash printing costs.
Secure your mobile workforce: By allowing companies to print securely via a simple touch of their smartphone or tablet directly to the printer, IT managers can ensure data printed through a secure mobile print environment cannot be compromised.

Protect your company paper trail: The most common printing security breach is the theft of a printed document resting in an output tray. By implementing a secure pull print solution, you can help your company decrease your risk of a data breach while also reducing printer waste.

Michael Howard is the Worldwide Security Practice Lead at Hewlett-Packard Company. In his leadership role, Michael Howard is responsible for evolving the strategy for security solutions and services in Managed Services. He works with the HP security business unit and labs to ensure HP’s leadership role in security, and also educates customers on the importance of security policies and procedures for imaging and printing. His primary area of focus has been around solutions for security, document management, core content management and output management.

Paul Ferguson

Of course the biggest mistake any organization makes when storing sensitive data is one of two things…

Either (a) Not encrypt it all, or
(b) Make some encryption implementation mistake that costs them dearly

Paul Ferguson (“Fergie”) is Vice President of Threat Intelligence at IID. Paul leads IID’s threat intelligence team that constantly collaborates with public and private enterprise to identify the latest malicious threats on the Internet. Ferguson has been widely...
recognized for decades as a security industry luminary and has been fighting malware since the days of the earliest attacks in 1987. Prior to IID as Senior Threat Researcher at Trend Micro, Ferguson evaluated the entirety of the technology landscape for security vulnerabilities, as well as tracked and correlated criminal operations on the Internet, communicating the latest variants of malware targeting the world’s largest businesses and federal agencies to law enforcement worldwide.

---

Jonathan Gossels

The biggest mistake companies make when it comes to securing sensitive data is…

The lack of understanding where their sensitive data resides because they have not set policies to systematically and consistently categorize their data, and consequently, they don’t have controls in place to ensure that all categories of data are handled appropriately.

For example, if a company has a policy that says any data set that contains personally identifying information is considered to be “sensitive” and has to be encrypted both in transit across a network and at rest, and the company has implemented technical controls to enforce that policy, it is very likely that the data set is safe.

There is also a user education dimension to this problem - users need to understand the sensitivity of the data they work with and their role in keeping it safe. In many cases, this involves educating users about what not to do.
For example, access to payroll data is usually restricted to those employees that process the payroll and those that review it. This is usually done within a payroll application that has built-in security and access controls. Payroll data and similar data sets should NEVER be downloaded onto an unsecure laptop, thereby undermining all the required controls. As in a very public data breach that occurred a few years ago, when this laptop was lost, millions found themselves risk for identity theft.

The best way to secure sensitive data is to do the basics well (like blocking and tackling in football). Understand what is sensitive in your data, set rules for handling it, implement technical controls to ensure it is actually handled properly, and educate your users about their role in keeping it safe.

Jonathan Gossels is the President of SystemExperts, a network security consulting firm specializing in IT security and compliance.

Amit Pamecha

Staying ahead of data security threats is hard enough, as seen in high-profile hacks of credit card numbers from Target and Home Depot the past few months. In my company’s opinion, brands need to get away from the business of having to store and manage credit card data and put it into the hands of experts. A business owner should be a business owner, not also a tech expert on top of that. That said, these are some tips companies should keep in mind when addressing their data security…
1. Train and staff up appropriately
   The training of a brand's people is crucial to data security. You need to educate every member of your organization about the significance of data like that, and you have to have a compliance officer involved in business decisions. When we work with very IT-savvy organizations, every decision they make, they ask, 'How does this affect PCI compliance or HIPAA?' Having somebody, an expert, assigned to that compliance helps.

2. Embrace new NFC methods
   More retail brands have developed their own smartphone apps with features like mobile pay and mobile loyalty, and they have taken major steps to make those apps more secure. Brands like Your Pie, Starbucks Coffee and Protein Bar, for instance, use branded apps that let smartphones communicate with special near-field communication readers attached to the cash register. When users enter their payment information into the app one time, it produces a special QR code the user can use to pay by holding it to the NFC reader rather than using a credit card. Apple's announcement of Apple Pay, an NFC system on the iPhone 6 that lets consumers pay with the wave of a smartphone, is most beneficial for retailers from the standpoint of its data security. Like other apps, Apple Pay lets consumers link their bank accounts to their phones by entering or scanning a credit or debit card. Importantly, however, the app does not save that account or card number and instead produces a unique code that a user may give to a merchant to draw money from the account. Transactions remain secure if the person using the account-linked phone is the rightful owner of the smartphone. Apple's security would go further by requiring the user to activate the TouchID, which verifies rightful ownership of the phone by scanning a person's fingerprint. Here, Apple is trying to remove personal info and get more to person-based authentication, which is the right way to be going. For franchise retail brands, it's something they should look at supporting as soon as possible, so that they don't have sensitive numbers store in their infrastructure.

3. Work with payment processors
   Though they do not have the same flash and cool factor as NFC from Apple Pay or QR codes, a major innovation coming soon to safeguard payment data are debit and credit cards with embedded "EMV" chips that authenticate users' identities and prevent fraud. Major payment processors like American Express have begun to roll out these smart cards as well, but there's been some foot-dragging on the retailer side investing in the technology needed to support them. It's not quite cool enough a tech leap to be on board with EMV chips right now, but if processors are asking you to do additional things, like require ZIP codes for purchases or support EMV, they often offer better terms on their transaction fees, so there are incentives to move that way.
Amit Pamecha is the CEO of FranConnect, a global franchise operating systems provider that helps franchisors sell franchises, manage franchise operations and franchisees’ local marketing. Services to businesses include franchisee royalty management, training, operations, marketing and e-commerce & POS solutions.

Dr. Scott Nelson

The single biggest mistake an organization can make in securing sensitive data is…

To trust its technology.

No matter how sophisticated, you can never trust your technology. In “The Code Book” by Simon Singh one of the best examples of this was during WWI when the Germans believed that they had impenetrable encryption and Foreign Minister Arthur Zimmerman sent the properly encrypted telegram that the British intercepted and then used to bring the US into the War.

Nothing is secure indefinitely and you are most vulnerable when you trust your technology unequivocally. Singh meticulously documented that anything that can be made secure will eventually be hacked.

So if you can’t trust technology, who do you trust? The short answer is yourself.
First, you must have a team that not only checks compliance with your security approach, but continuously monitors the actions of the hackers and constantly upgrades your approach securing sensitive data. But this is only the beginning of the solution. Your MarComm organization must also be ready when the inevitable happens.

When iCloud was recently hacked, Steve Cook did not come out with a letter that focused on a new technology approach to iCloud security. He quickly assured people that the hole was fixed and then spent the majority of his time stressing the company values toward the concern of Apple’s customers: privacy. You must have a planned response to address what matters to your customers. In Apple’s case this was privacy. In the case of a bank it is limitation of financial liability. In the case of home automation it will be assurance of safety. Don’t make the mistake of trusting your security technology unequivocally. Be technically prepared and diligent, but know that it will fail and be prepared to protect the brand and maintain customer trust.

So start with the assumption that a motivated party will get access to your data. Now what do you do. Updates. Change in operational processes. Minimizing footprint and signature. Never let guard down, updates, patches, research. Partner and collaborate.

Dr. Scott Nelson is the CTO and Executive Vice President at Logic PD. In his leadership role, Dr. Nelson responsible for leveraging Logic PD’s technology expertise and offerings across a wide range of markets with a focus on connected solutions and the Internet of Things (IoT). Scott has nearly 25 years of experience leading technology and product development.
Jack Wilson

The biggest mistake companies make when securing sensitive data is to…

Underestimate the necessity of managing their software vulnerabilities!

The lack of endpoint security is among the biggest corporate security threats. And vulnerable software on these endpoints is one of the most popular attack vectors with hackers – an attack vector that is likely to become more and more used.

Gartner predicts that in 2015 80% of successful hacks will succeed using known exploits. These attacks can be deflected if the organization ensures that the applications on their network are patched and up to date, and that every vulnerability is remediated or mitigated. It is essential that companies take preventative action against vulnerabilities, which can affect both hardware and software on the network.

Essentially, business and private endpoints are very rewarding targets for cybercriminals. This is because, being extremely dynamic environments with numerous programs and plug-ins installed, they are very difficult to secure. Together with unpredictable usage patterns, this makes them formidable targets that are difficult to defend.

Endpoints are where the most valuable data is found to be the least protected. By definition, endpoints have access to all data needed to conduct an organization’s business, and every endpoint represents a valuable target for cybercriminals, even if no sensitive data is present. The endpoints computing power and bandwidth provide valuable resources, for example as an infection point, proxy, or for distributed password cracking services.

To protect endpoints that are connected to the corporate IT infrastructure from vulnerabilities, it is essential to identify the vulnerable software, prioritize it and when possible patch it. A patch remedies the root cause of the problem, and thereby eliminates a large number of attacks. Where a patch is not available, other mitigation methods must be applied.
To summarize: the complete visibility of an organization's infrastructure - and receiving verified vulnerability intelligence - is essential to securing sensitive data. By constantly monitoring the corporate environment, companies are able to pinpoint where the dangers lie and tactically prioritize their remediation efforts.

Jack Wilson is Vice President and General Manager of North America for Secunia, a provider of optimal security and vulnerability management for enterprise customers and home users, where he drives the company’s North American sales strategy, execution and expansion.

Colin Lobley

The #1 biggest mistake companies make when it comes to securing sensitive data is…

Not valuing the data to enable risk-based investment.

When faced with data security, most businesses reach for a cyber-/IT-security standard and look to the IT security manager / CISO / CTO to implement this. This has the potential for businesses doing too much or too little when it comes to securing their data - security standards are a 1-size fits all approach but individual businesses are anything but standard. Their operating environment, the threats they face and their risk appetite will all be different.

To be able to accurately invest the right amount in the right areas to secure data in a way that enables risks to be managed in line with appetite, businesses need to be able
to undertake a robust risk assessment and in turn develop a robust business case for targeted investment.

Best practice suggests that organizational objectives (KPIs), risk appetite and risks should all carry the same unit of measure - typically £/$/other currency in a commercial organization. Assessing the business impact from the threats to sensitive data in these terms is not a common practice. In the traditional 'reach for a standard' approach the important step of identifying the relative value of data and information in terms of its contribution to operational delivery, and ultimately strategic objectives is not undertaken with the level of robustness needed to accurately assess the business risk and make a business case with clear ROI assessments.

A risk-based business case is typically invest £/$ 'x' to minimize the risk by 'y'. If the data is not valued in financial terms, the risk cannot be assessed in financial terms, and so 'y' cannot be assessed in financial terms and the ROI becomes unclear leading to under or over-investment.

Colin Lobley is a director at London-based strategy and risk consultancy Manigent, where he heads up the Information Risk Practice working with businesses to help them build competitive advantage from their information and cyber-resilience.

Michael Fimin

When it comes to securing sensitive data, the biggest pitfall hides in…
The false confidence that you know exactly what is going on across your IT systems.

If all IT pros know exactly what is going on in their IT infrastructures, so why do companies continue to experience security incidents that are discovered months after a breach occurred? “2014 State of IT Changes Survey” found out that more than a half of IT professionals still make changes to their IT systems without documenting them. Obviously enough, this makes the detection of the data leak source a difficult task, as there is a huge number of changes happening to data and system configurations.

When a user accesses the data, downloads or shares it - all these activities are tracked in the log files. When there is a decent amount of users working with sensitive information, monitoring those changes manually becomes an uphill task that will most likely lead to overlooked malicious change that caused a security breach. Assuming that the data is under rigid control without any proof, unfortunately, you put sensitive information at risk. So a wise thing to consider will be establishing a continuous auditing of the entire IT environment.

Change auditing solutions that give real-time information of unauthorized or malicious changes help you ensure a complete visibility across your IT infrastructure, prove that security policies in place actually work and sensitive information is secured. This will not save you from security violations, but will help to detect a breach on early stages, assist during root-cause analysis, and therefore indicate weaknesses that you can fix to strengthen security of your IT infrastructure.

Michael Fimin is the CEO and Co-Founder of Netwrix, #1 provider of change and configuration auditing solutions.
Joe Moriarty

The #1 biggest mistake companies make when it comes to securing sensitive data is…

Not adding security layers to data shared in the cloud.

The popularity and skyrocketing adoption of cloud-based file sharing and storage services have made it easy for businesses alike to collaborate and share content with multiple users. As businesses turn to cloud storage and sharing platforms such as Google Drive, Dropbox and others, data leaks become an increasing concern. These services lack the security controls required to mandate and track with whom, how and when file and content are shared.

By adding content controls, protection, tracking and deep analytics to files, companies can plug security and workflow holes. Content controls enable companies to address security concerns by adding watermarks to files and videos; limits on file viewing, printing and forwarding; engagement and activity analytics; and more - preventing unauthorized access to data, screenshot taking, credential sharing, and other data leakage risks.

Joe Moriarty is Co-founder of Content Raven, a cloud based content control and analytics platform, and has a long history of motivating teams and delivering increased sales for various technology providers. He co-founded Content Raven in May 2011, previously working with Hybrivet Systems, where he was Vice President of sales and marketing. Joe holds a Bachelor of Science in Resource Economics from the University of Connecticut.
David Arnoux

The #1 biggest mistake companies make when it comes to securing sensitive data is…

They simply don't take the time to secure devices and data that are physically "leaving the building".

Nowadays many companies distribute laptops, tablets and smartphones enabling employees to work any time, any place. Instead of coming to work to work on fixed desktops, the employee is taking work and company data everywhere (physically).

This once secure data leaves the secure company building and can be:

- exposed to being stolen or loss
- being used by others (children or spouse)
- being used at home for online shopping etc.

David Arnoux is head of growth at Twoodo, a team collaboration tool for the #hashtag generation. Building SaaS products and meeting with CTOs weekly has made him an expert in understanding customer security requirements.
Alan Baker

In my opinion, the biggest mistake companies make when it comes to securing sensitive data is that…

They minimize or ignore the human dimension of security; there is a cultural aspect to security that must become part of the DNA of the organization.

Organizations are willing to spend a lot of money developing the necessary standards, guidelines and procedures required by a comprehensive security program, and they are willing to spend even more on the technology required. Where organizations tend to drop the ball is the human element; staff needs to be acutely aware of the security policies, trained in the proper application of the policies and understand (and accept) their personal responsibilities and accountabilities. There needs to be a training regimen for both new and existing staff, as well as periodic refreshers. Security responsibilities should be built into their role descriptions and their personal objectives.

It’s also necessary that security be deployed in a manner that will allow staff to fulfill the responsibilities of their job while fully complying with the requirements of the program. The information security program cannot be a roadblock; its application must be proportional to the risks identified and it must support (and not inhibit) the ability of the organization and (and its staff) to conduct its business.

And a second mistake: Organizations implement a security program and think they’re done. They’re not. Security programs need to continuously adapt to in order to meet new threats and environmental changes. The security landscape is ever evolving, both
on the side of threats and on the side of regulators; organizations need to ensure that their security programs change in response.

Alan Baker is the Owner, President and Chief Consultant at Spitfire Innovations, a boutique consulting firm based in Toronto, Canada, that helps organizations envision, prepare for and implement change. The business specialties include financial services, particularly life insurance, and customer relationship management. Prior to his leadership role at Spitfire Innovation, Alan was an IT AVP at a medium size life insurance company where part of his portfolio was IT security, and where he was responsible for the creation and maintenance of the organization's security program.

Stelios Valavanis

There are lots of things companies neglect when securing their data. The biggest one is...

A lack of monitoring (IDS) and reporting to a tight control matrix.

Without it they never know if their policies are even being adhered to. On top of that the process has to feed back findings into the IDS signatures. These internal policies and their measurement are the biggest security exposure.

Stelios Valavanis is the Founder and President of onShore Networks. He currently serves on the boards of the ACLU of Illinois and We the People Media, and advisory committees for several other organizations. He has appeared as a guest lecturer and
panelist for local colleges, non-profits, and various industry events. Stelios graduated from the University of Chicago in 1988 with a Bachelor’s degree in Physics. Prior to founding onShore, Stel held a number of technical positions at the University of Chicago.

---

Eric Jeffery

When it comes to the biggest mistake companies make when it comes to securing sensitive data, there's a very simple answer…

They don't!

Businesses "believe" they are securing data, yet, sadly, they are not. There's a huge discrepancy between what IT says/thinks they are doing versus what leadership understands. Usually through ignorance, sometimes through negligence.

This lack of securing data occurs through failure to backup active systems to failing to verify if the backups are viable. They don't understand the difference between data in transit versus data at rest and the fact there's need to handle each in separate fashion.

I had a hospital client that had not backed up their financial system for 7 years. I had a global SAN storage company that almost burned down 2 years in a row and all of their data was in the same room on two different storage devices. I had another hospital client that backed up their critical systems to tape and stored the tapes in the same
room as the server. These all go to complete lack of security the data. Not to mention none of the backups, on tape, that’s transportable, were encrypted.

Eric Jeffery Founder and CEO of Gungon Consulting, a firm with focus on small and medium sized business. Our services provide assistance in the critical areas of cyber security, system availability, off-site infrastructure solutions as well as operational efficiencies and productivity enhancements for our clients. Eric has over 15 years' security experience including work for the DOD, healthcare industry, aerospace, and numerous technology companies.

Jeremy Ames

The #1 biggest mistake companies make when it comes to securing sensitive data is…

Differing standards of data security.

More specifically, in most companies, executives are held to a lower standard of data security than the rest of the employee base. They’re allowed more leniency in terms of BYOD and in general they operate more freely outside the corporate firewall, which is a huge mistake.

The reality is that if a group is out there trying to plan a cyber attack, they’re most likely to target a member of the C-Suite, particularly the CEO, because they know he or she is going to be the holder of the most sensitive information.
That means that executives need to be even more diligent than the rest of the employee base, because if information is compromised it could have damaging financial and legal ramifications. That being said, most companies fail in the three-pronged defense necessary to protect executives:

1. additional focus by IT
2. continued education by HR and
3. personal responsibility by the executive

Jeremy Ames is President of Hive Tech HR, a technology consultancy that helps companies find, implement and enhance their HR systems. He is a member of the 2014 SHRM HR Management and Technology expertise panel, and former CFO of IHRIM, an association for Human Resources Information Management. Jeremy has been quoted in many articles dealing with the securing of HR data, including a SHRM article entitled "Prevent CEOs, C-Suite Executives from Getting Hacked" and a recent article about the Backoff virus.

Steve Marsh

The greatest security mistake organizations make is…

Failing to protect their networks and data from internal threats.

“Snowden" has become the buzzword for every kind of security breach. But the Snowden leak was an inside job.
The leak was the result of a SharePoint-related issue – not with the SharePoint platform, but with governance decisions (i.e., who has access to what data), monitoring and oversight. In Snowden’s case, he copied gigabytes of data to thumb drives with little challenge. Snowden was given access to sensitive content that he shouldn’t have had access to for the purpose of carrying out his tasks. He was already inside the fortress.

Somewhere along the line, the security and governance protocols broke down within the NSA and Snowden was able to access and take sensitive data. The NSA may still not be entirely sure what content was copied. Pro-actively addressing the insider threat with appropriate security and controls would have made it easier to properly assess the damage. The problem will only grow if government agencies and businesses use the same security and governance protocols as they go to the cloud or use a hybrid (cloud and on premises) model.

The challenge for government and business is to use the tools that SharePoint and vendors like Metalogix provide to pro-actively establish, monitor and enforce security protocols and to limit internal access to sensitive content.

Steve Marsh is the Director of Product Marketing for Metalogix, providers of industry-recognized management tools for mission-critical collaboration platforms. For over a decade, Metalogix has developed the industry’s best and most trusted management tools for SharePoint, Exchange, and Office 365, backed by our globally acknowledged live 24x7 support. Over 14,000 clients rely on Metalogix Tools every minute of every day to monitor, migrate, store, synchronize, archive, secure, and backup their collaboration platforms.
Credit card data is one common type of shared sensitive data for many companies that affects businesses and consumers. Nearly every major attack against credit card data in the past few years has exploited a single, glaring vulnerability in the current payment industry infrastructure…

The fact that merchants are still permitted to handle actual credit card data in their systems. The industry security standards (PCI DSS) and even the card brands’ best practices have failed to protect merchants from these types of attacks. It doesn’t have to be this way.

The current mindset of most payment security “experts” is fundamentally flawed. They are focused on rules and regulations to protect data that merchants shouldn’t have in the first place. These payments industry regulators want businesses to pay to dig deeper moats and build higher walls around their castles in order to protect the princess (the sensitive data) inside. Wouldn’t it be simpler (and more cost effective) to remove the princess from the castle and move that vulnerable data to a location purpose-built to protect sensitive data?

This is exactly what happens when merchants properly combine point-to-point encryption and tokenization technologies. With encryption occurring as soon as the card data is swiped (or keyed in), the business never handles actual card data as the transaction is processed through the merchant environment. And with only a secure token returned to the merchant along with the authorization, there is no more risk of storing vulnerable cardholder information because the onsite database only holds tokens that are meaningless and valueless to thieves.
As an added bonus, this approach of combining point-to-point encryption and tokenization drastically reduces the amount of vulnerable data in the merchant’s environment, which in turn reduces the scope of their annual PCI assessments - saving time and money.

Dave Oder is the President/CEO of Shift4 Corporation, the world’s largest independent payment gateway. A relentless advocate for merchants, Dave introduced tokenization to the industry in 2005 and released the technology without patent so that other vendors could likewise leverage it to secure their merchant customers’ data. Dave earned a Bachelor’s in Business/Accounting, a Master’s in Computer Science, and an MBA - all from University of California, Los Angeles.

Ivo Vachkov

In my experience #1 security mistake companies make is…

Relying on obsolete security models in complex IT environments.

Many companies would just keep using their well established systems with no concern for the changing security landscape, following the well know “Don't fix it if it ain't broken” concept. And that complacency is usually the reason for the downfall.

Increasing IT Complexity in combination with obsolete technologies are a dangerous mix. Avoid it if possible, or adjust if not. This is where IT security personnel should add value to your organization.
In many cases different security models cannot even co-exist. Due to time pressure engineers will follow "least resistance" path choosing to lower the security requirements, instead of reworking the whole component, thus introducing security flaws in the product in the implementation phase.

There are cases where this situation looks unavoidable (old IT infrastructure supports only obsolete crypto technologies and you still need to work with it). It is usually not. One can always use security in depth, different forms of perimeter protection, service isolation and compartmentalization techniques to "upgrade" to a modern security level.

In any case, be aware that increasing IT complexity, natural human complacency and the "least resistance" are serious enemies to data and system security.

Ivo Vachkov is DevOps Engineer in Xi Group Ltd, where he deals with data security concerns on a daily basis. In the past he worked as Head of IT for the biggest prepaid MasterCard card issuer in Europe. He is also teaching "Programming Secure Code" and "Network Security" courses in New Bulgarian University in Sofia, Bulgaria.

Andrew Bagrin

I believe the #1 biggest mistake companies make when it comes to securing sensitive data is…

Relying on the big misconception that if your data is stored in the cloud, it is less secure than if it’s not stored in the cloud.
Without look at how much data was stolen from the cloud versus local computers and servers (because it's just too hard to track) we can look at it theoretically. If you store data on your computer or server and that computer is connected to the internet somehow, you are now part of “the cloud."

So the question becomes, do you feel that you can secure your data locally better than the experts at Google, Box, Dropbox etc.?

Do you know the ins and outs of stored data security?  
Do you keep everything up to date, protected etc.?  
Or should you rely on the experts?  
Do you keep your valuables in a safety deposit box, or at home under your bed?

The news of Apple iCloud and Jennifer Lawrence make us doubt the cloud, it’s just that we don’t hear about the hundreds of cases where data was stolen from local computers.

Andrew Bagrin is the CEO and Founder of My Digital Shield, a leading provider of Security-as-a-Service (SECaaS) for small businesses, and an IT security expert with more than 17 years of experience.

David Mohajer  
The number one mistake that companies make when securing sensitive data is…

Not contemplating and reconciling the human element.
1. What do you do in the case of corrupt employees? How do you know who it was that breached your data? We solved this by making the data unique to each person so we can figure out who disseminate what in the event of a follow-up to the breach.

2. Lazy employees who may not understand how to handle the data properly (they need to understand what Protected A is vs. Protected B, etc.) or are too lazy to do so. You can solve this by training them and re-engineering the related systems (if feasible) to make them more convenient to use for lazy users. A lazy employee might even be a manager who is assigning roles or privileges to their team - they need to understand that only specific things should be assigned. Example: Giving everyone administrator rights to a critical system when they only need to enter in work orders is opening the doors for trouble.

3. Not having a process in place to detect problem employees, and problem vendors that have partial access to your systems. Example: Someone in your office sets up a man-in-the-middle attack (easy to mitigate/detect if you prepare for it) on your server, but you don't have a process in place to verify that traffic is routing properly. They can get away with a lot of sensitive data without anyone knowing until the damage is done.

David Mohajer is Chief Executive Officer and Co-Founder of XAHIVE, a Canadian social networking platform that facilitates mass communication between people within a 2-kilometre radius. In his leadership role, David has a clear vision for the future of XAHIVE, and has been implementing the plan with the help of the Chief Operating Officer (COO), Sem Ponnambalam, since September 2013. David has fifteen years of experience working as an information technology consultant in the private and public sector, and an additional five years of experience working as a federal government employee.

---

John Dancu
The #1 biggest mistake companies make when it comes to securing sensitive data is…

Not having a robust identity verification system in place when verifying someone in a customer not present environment.

John Dancu is the President and CEO of IDology, a provider of innovative technology solutions, where he has served since 2005. During this time, IDology has grown to be a leading provider of identity verification and fraud prevention solutions in the financial services, merchant processing, payments, retail, healthcare and other markets.

Christopher Stark

Accessibility to information anytime and anywhere makes the cloud an attractive option for companies looking for assistance with storing sensitive data. Before a company decides to store critical information in the cloud, there needs to be a level of trust with the cloud vendor it chooses. The biggest mistake companies make when deciding to store sensitive data in the cloud is…

Choosing the wrong vendor.

An error in judgment or shortening of the vetting process of prospective cloud vendors can leave a company vulnerable, because information thought to be secure could actually be accessed by hackers. Often times, companies face issues related to security and accessibility when it partners with a cloud vendor that does not confirm where the
data will be stored. This could lead to increased retrieval time for information or data breaches in the most extreme cases.

The ideal vendor for a company is a solution provider that stores information off-site in a U.S.-based data center that is under lock and key, physically and logically. From the data center, the cloud vendor will have the capability to transmit sensitive data to a company's headquarters, satellite offices or to staff members working via the cloud using 256 bit encryption. The cloud vendor will have security protocols in place to ensure or restrict access to information as appropriate and the IT staff overseeing the data storage and retrieval processes will undergo thorough background checks.

When a company partners with a cloud vendor it trusts, it can rest assured that sensitive data is secure. Companies can save themselves from making the critical mistake of choosing the wrong vendor by simply doing their due diligence. This involves checking references, confirming with prospective vendors where data is stored and the lengths they will go to physically and philosophically protect relevant information.

Christopher Stark is the President and CEO of Cetrom Information Technology, Inc., an industry-leading provider of custom cloud solutions. A veteran of the IT industry with more than 25 years of experience in all facets of the IT industry, and holding some of the industry's most prestigious technical certifications, Stark founded Cetrom in 2001 based on the premise that there was a smarter, easier way to conduct business.
The biggest mistake we see businesses—especially SMBs—make when securing sensitive data is…

The hope strategy.

It goes something like this. We lock our filing room, have a password policy on employee computers, and use a firewall on our network. We hope that’s enough to keep out the bad guys. Besides…why would anyone want to come after us?

Here are the facts. The number of incidents reported in the last 12 months rose 25%, and the average losses resulting from these breaches rose by more than 18% [1]. The hope strategy simply isn’t working. You have to think beyond just electronic data to also protecting confidential information stored on paper as well.

We encourage companies to take a look at Enterprise Content Management (ECM) systems like Digitech Systems, Kofax, and Hyland. These options are lower-cost, so they’re within reach for companies of all sizes. ECM also includes better data security than many IT departments can offer. ECM converts paper to electronic images, which are stored in the same secure repository as electronic files. For those with permission, information is available using a simple keyword search. Everything is protected by multiple layers of protection like passwords, SSL, and encryption at rest and in transmission.

ECM is available as both traditional software to install on your corporate network or as a cloud-based service. To further boost your data security when choosing cloud ECM, ask for the SOClII audit report to verify the provider’s system controls meet your needs.

ECM offers additional benefits besides control. A report released this week from Nucleus Research indicates that every $1.00 invested in ECM technology will return $7.50 to your organization in value.

HK Bain is the President and CEO of Digitech Systems, providers of an Enterprise Content Management Solutions Software, and oversees the management and overall vision of the company. Shortly after joining the company in 2000, he implemented the company’s Foundation, which guides decisions, strategic planning and business growth based on organizational values and priorities. Standing firm on his priorities of God,
family, and work, Mr. Bain attributes his success to maintaining a value-based company that weighs all activities against this strong set of guiding principles.

Amit Bareket

In response to the question of “what is the #1 biggest mistake companies make when it comes to securing sensitive data”, I have a few words of advice…

First of all, many companies store their clients’ passwords as plain text rather than hashed passwords. That is very risky since all their clients’ data gets compromised in the case of a security breach. Since many people use the same login names and passwords for all their e-mail and social media accounts, hackers then get instant access to all the users’ accounts in such a leak.

Studies have shown that the average cost of a data breach is US$3.5 million, so it is obvious that companies must focus as much on securing their own data as they must safeguard their clients’ data (source: 2014 Ponemon Cost of Data Breach: Global Analysis).

A second, yet related, mistake is that some companies don’t use any kind of encryption when sending confidential data over public and non-secured networks. This means that a snooper on that hotspot can intercept all unencrypted transmitted data, including passwords. There is then a possibility that the snooper can use those intercepted credentials to log into the company’s business systems, cloud storage or intranets.
To mitigate this risk, companies must ensure that all their employees always connect using a virtual private network (VPN) which encrypts the user’s connection and prevents hackers from snooping into any transmitted data. On top of that, all devices should be secured with anti-malware software to prevent the spread of any virus or malware.

Amit Bareket is the CEO and Co-founder of SaferVPN, a VPN provider that helps thousands of individuals and dozens of enterprises worldwide safeguard their private data online. Amit has over 10 years of experience in cyber security, including the role as Team Leader at IBM, and has 7 patents pending in network technologies and file storage. SaferVPN works proactively to educate people on the importance of online security and privacy, making it easy and accessible to everyone, everywhere.

Patrick Oliver Graf

The biggest mistake companies make when it comes to securing sensitive data is…

Failing to have a defense-in-depth strategy in place.

As user demand for BYOD and remote access increase, enterprises should look for a better approach - one that includes multiple lines of defense - to keep their sensitive data and networks secure.

Taking precautionary measures to mitigate the risks associated with corporate data, especially when being accessed remotely, should include a user-centric, centrally managed VPN. By using such a solution, enterprises can guarantee that sensitive
information remains secure, while allowing employees access to the corporate network using any device.

Further, by focusing on employee education programs, creating common sense BYOD policies and implementing best-of-breed, interoperable solutions that help to secure corporate networks, BYOD can be supported while minimizing network security risks.

Patrick Oliver Graf is CEO of NCP Engineering, and an industry veteran with more than 19 years of experience in technology product management. His company sells its remote-access VPNs to government agencies and other organizations, providing technology for fast, secure access to their network resources and communication of sensitive data.

Chuck Davis

The biggest mistake companies make when securing sensitive data is…

Not properly classifying it and protecting it against current threats.

There are three essential parts to proper protection of sensitive data.

1. **Data Classification** - Companies must understand what data needs to be protected and create a Data Classification Policy to classify data based on sensitivity. At a minimum three levels of data classification are needed.
   - **Restricted:** This is the most sensitive data that could cause great risk if compromised. Access is on a need-to-know basis only.
Confidential or Private: This is moderately sensitive data that would cause a moderate risk to the company if compromised. Access is internal to the company or department that owns the data.

Public: This is non-sensitive data that would cause little or no risk to the company if accessed. Access is loosely, or not, controlled.

2. Encryption - Encryption is a very generic term and there are many ways to encrypt data. Companies need to implement and manage encryption correctly. The key to a good encryption strategy is using strong encryption and proper key management. Encrypt sensitive data before it is shared over untrusted networks (ex. Encrypted Email, Encrypted file storage).

3. Cloud Misuse - Storing data in the Cloud equates to storing your data on someone else's computer. Once it's there, you no longer have control over it. If that data is Classified or sensitive, encrypt it BEFORE uploading to the Cloud. If you will be sharing keys with the Cloud provider, make sure you understand the Cloud provider's policies. (ex. What is their backup policy? Who has access to your data? What's their data breach communication policy?)

By understanding what you're trying to protect, and creating a strategy to protect each level of data appropriately, companies can adequately secure data against the threats of today.

Chuck Davis, MSIA, CISSP-ISSAP is an Author, Professor and Senior Security Architect. He teaches Ethical Hacking and Computer Forensics classes for Harrisburg University and is a Senior Security Architect at a Fortune 500 Company, having previously worked as a Security Operations Manager for IBM. He holds the CISSP and ISSAP certifications from (ISC)2. He also co-authored two books on the subject of security, holds four patents and has four published invention disclosures. He has been a speaker at numerous security conferences and was a featured guest speaker a Hacker Halted Conference in Mexico City and Atlanta, GA.
The biggest mistake companies make when it comes to securing sensitive data is:

Not paying enough attention to social engineering.

Social engineering nowadays is the best way to obtain sensitive data. There are no long passwords, no two-factor authentication, no firewall, no virus program, just people.

People can be hacked easier than security systems, I could send 100,000 emails to a company to try and break through their spam filter or I could make one phone call to the receptionist and use some expert social engineering techniques and retrieve data and/or sensitive information.

Social engineering is definitely easier than trying to crack security. A polite phone call can get your desired results in a matter of minutes and social engineering is used more and more every day to obtain sensitive data.

Liam Fallen is the Founder of MonthlyWebs. Liam has previously successfully used social engineering techniques in a positive way to influence business leaders and to raise funds for various charity fundraising efforts.
Fax is the most commonly forgotten, but most reliable and secure method of document transport, and in my experience, one of the biggest mistake companies make when it comes to securing sensitive data is:

Not utilizing the method of faxing for securing sensitive data in their document transport.

Faxing is secure because a faxed document is transmitted as an image file, and as a result the data in the document cannot be edited or decrypted. Viruses cannot infect your network from a fax, because they cannot be embedded anywhere. A faxing technology that operates in the cloud allows for companies to easily cut down costs and scale their secure fax operations.

Paul Banco is CEO of etherFAX, a unique service that extends existing fax server solutions to the cloud. By eliminating the need for costly network fax systems, such as fax boards and recurring telephony fees, etherFAX leverages the Internet to manage all business-critical fax communications.
Drew Farnsworth

The biggest mistake companies make when it comes to securing sensitive data is...

Not updating their passwords and access.

I'm a data center infrastructure designer and consultant. When designing, building and commissioning data centers I have more than once been given access to the internal network of a company. Months later I have come back and the passwords were not changed. I have always asked that this access be restricted.

In the wake of Edward Snowden it has become increasingly obvious that contractors of all kinds are given access to valuable data systems for a longer duration than they should be. User management controls should be put into place in order to guard against outside contractors who (unlike me) might take advantage of the critical infrastructure that they either installed or maintained.

Drew Farnsworth is a Design Lead at Green Lane Design LLC, a firm that provides Data Center Design solutions, and has been working in the Architectural Design industry for over ten years. He has experience with uninterruptable power systems, N+N distribution and redundant generator systems and in the past six years he has undertaken numerous investigations into data center growth and reliability plans for Fortune 500 companies.
Rich Reybok

From my perspective, it's not that organizations are using the wrong technologies, perhaps the wrong key management or approach to encryption, or even wrong approach to classification of their data. The biggest problem that I see organizations make with securing sensitive data is...

Not being able to even answer the question of what the lifecycle of their data is.

They don't know if all of their data is actually protected in the first place, as they may not even know where it all is and what routes are available to access the data.

As we transition to the so-called "3rd platform" based on cloud, mobile, and social, it's increasingly impossible to track all the data through its lifecycle. Do organizations have an inventory of all their repositories that is kept up to date? Do organizations know where all their log data is stored and who can manage it? If they know where the data is stored, do they have an accurate picture of all the people and services that are able to access the data? Do they have all the proper policies and procedures in place to access the data?

The problem is it only takes a single instance of something not following the best practice for data security to break down. Attacks are often about escalating knowledge. If sensitive information about how the data is stored or accessed can be gleaned from a mobile app by reviewing the log stream over my USB port, then the whole model falls apart. The threat actor takes what he learns from the app log and uses it to escalate to your endpoint API or your data services, looking for the next leak that gets them closer
to the repository. Failure to know where all the data is stored and its touch points can lead to a disastrous chain of events.

Rich Reybok is the CTO and SVP of Engineering of Vorstack.

Aaron Ross

The biggest mistake companies make when it comes to securing sensitive data is...

Not doing the proper research.

Every company requires a different solution to secure its data. A hardware company needs a cloud solution that lets them track mainly inventory online, whereas a small pharmacy needs to be able to communicate with their customers privately through a secure cloud portal. Each company needs a different data solution and it would be a tremendous mistake to choose a company without doing intensive research.

Ultimately, choosing a payment provider makes all the difference when it comes to dealing with sensitive data, customer or company. With the Home Depot data breach, their mistake was not having a separate company monitor the credit card software. Instead of having Symantec monitor their information, they left that endpoint setting off, resulting in the breach.

However, a smaller company would not need to institute such heavy protocols. Sanjiv Beri, President of Priority Payments Systems in the Northeast explains, “Having highly
encrypted information using a reputable gateway is key to keeping customers information secure.” Signing up your small business for credit cards payments through an unknown online company not only can put your company and customers at risk, it'll cost you more as well!

What it comes down to is: understanding what information you need protected. Once you have that settled, you can make a determination of what company can best help you keep this information secure. Get references, find out if this company has ever had a software breach, and make your educated decision. A little research now can save you a lot of heartache later.

Aaron Ross is an Internet Security Expert and Owner of the cloud site RossBackup.com. You can often see Ross talking about internet security on Fox News, CW & ABC, among other places.

---

Ryan Satterfield

The biggest mistake companies make when security sensitive data is…

Not understanding what their own code truly does and how other code in their system actually works. It’s one thing to write code, but even the largest companies underestimate how their program can be used by an attacker.

One good example is the bug in Bash that the public has been alerted to. Every company that updates their server to protect against remote attacks now believes their
server is secure. This is not the case. The patch for the bash bug is easily bypassed, so even so-called patched servers are still exploitable. We have exploit code for the latest version of bash that works, but don't believe it would be appropriate for it to be published at this point in time.

Non-security companies don't fix bugs that they don't understand even when they have a major impact or when they make the mistake of believing a bug is minor. Underestimating bugs is a fundamental mistake that even the largest companies make. A bug can seem minor, but attackers know how to make "minor bugs" have a major impact and use that to steal user information.

I can sum up companies and security with one word: underestimation – that is the underestimation of what their code can really do in the hands of an attacker.

Ryan Satterfield is the Owner and Founder of Planet Zuda, LLC., a security company that has assisted Google, Ebay, Inc., Godaddy, and several other recognized technology companies. Ryan has personally been working with online security since the mid 90's and has worked in the field of Internet security professionally since 2007.

Kevin D. Murray

This is a great question and my advice comes from almost 40 years of experience. The #1 biggest mistake companies make when it comes to securing sensitive data is...

Tunnel vision focus on IT security.
All pre-computer era information theft tactics still work, and are still used. And, most "computerized" information is available elsewhere before it is reduced to data.

Effective information security requires a holistic protection plan. IT security is an important part of this plan, but it is only one door to your house of information.

Here is The Holistic Approach to Information Security

1. Begin by protecting information while it is being generated (discussions, audio and video communications, strategy development).
   Conduct Technical Surveillance Countermeasures (TSCM) inspections of offices and conference rooms on a scheduled basis. Ford Motors found voice recorders hidden in seven of their conference rooms this summer.

2. Protect how the information is transmitted (phone, teleconference, Board meetings, off-site conferences).
   Remember, wiretapping and infiltration are all still very effective tools. Check for wiretaps on a scheduled basis, or encrypt the transmissions. Conduct pre-meeting TSCM inspections. Never let presenters use old technology FM wireless microphones. They broadcast further than you think.

3. Protect how information is stored.
   Unlocked offices, desk and file cabinets are a treasure trove of the freshest information. Print centers store a copy of all print jobs. Limit written distribution of sensitive information. Crosscut shred sensitive waste paper. All these vulnerabilities and more should be covered during the security survey portion of your TSCM inspection.

4. Educate the people to whom sensitive information is entrusted.
   Security briefings don't have to be long and tedious. Establish basic rules and procedures. Explain the importance of information security in terms they can understand. "Information is business blood. If it stays healthy and in the system, your job, and chances for advancement, stay healthy."

Kevin D. Murray, CPP, CISM, is a TSCM specialist providing electronic/optical surveillance detection and counterespionage consulting for business and government. New York area headquarters, with services available worldwide. Learn more about Kevin and his work at [www.counterespionage.com](http://www.counterespionage.com).
Mark Nicholas

As an attorney who has practiced law in the financial, data and tech fields for more than 2 decades, and now as the founder of a company dedicated to securing people’s data, it is my opinion that the core risk to securing sensitive data is…

In the control over admin passwords as well as in the manner in which customers address their affairs.

More breaches are caused by simple password intrusion than any other method and it can be a nightmare convincing customers to take even the most basic self-protections. On the admin side, the ability to log in with access to the overall records of the company is likely the most significant cause of major breaches that exist; all could be easily prevented.

Mark Nicholas is the President and CEO of Family Archival Solutions, Inc., a company committed to offering a variety of state-of-the-art services to help prepare for, prevent, and address the most important issues facing your family, primarily by protecting personal legacies, family assets, and important documents.
Matthew Turner

One of the most dangerous aspects to how many management systems or individual organizations approach the management of secure data is…

The simple use of (and reliance on) network drives.

It may seem easy to store your documents, PDFs and other files on a network drive because it is easy to set up file sharing. But all you’re really doing is replacing paper file cabinets with electronic files cabinets, and you still face all of the issues you faced before with security, hours spent searching through folders, managing issues with former employees and audits.

As a specific example of how this can affect a company, if documents can be altered on a network drive they are no longer legally admissible. Regardless of your industry or the regulatory landscape you face, every organization faces legal threats. Any civil action or lawsuit proceeding you might face in the United States is subject to the Federal Rules of Civil Procedure (FRCP). FRCP requires that every company involved in a lawsuit or federal litigation must safeguard and access electronic documents and email messages as part of the discovery process.

That means all documents archived on your servers are subject to legal discovery. You must preserve those documents in an unalterable form as evidence, including correspondence outside of your management system. The risks of noncompliance include steep fines and even criminal penalties.
Matthew Turner is Chief Marketing Officer of PaperWise, a workflow automation and enterprise document management solutions provider focused on adaptable and scalable solutions to clients ranging from small firms to Fortune 500 companies. Matthew is also the Founder of the a corporate strategy and marketing firm, Boston Turner Group, and has worked with dozens of hyper-growth companies ranging in size from $20M to $12B in annual revenue helping to set corporate marketing strategies that develop, build, and accelerate value capture in differentiated markets for sustained growth.

---

**Comments (1)**

Pam | October 08, 2014 3:51 pm

Very interesting article. The lack of understanding where sensitive data resides mentioned by Mr.Gossels is particularly true to many organizations.

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 \( \ast 3 + 11 = \) 

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