Don’t Get Hacked: What Every Executive Should Know About Data Security

Author, Chris Tomlinson

A Peppersack White Paper

December 2015

---

www.peppersack.com

Don’t Get Hacked: What Every Executive Should Know About Data Security by Chris Tomlinson

Introduction to Data Security

In today’s business world, your company cannot survive (let alone thrive) without an online component. A static website and social media presences are the very minimum requirement for businesses to make it in the twenty-first century. Even this, however, is becoming too little for most companies. Thanks to Amazon and other online marketplaces, if you do not have a means to sell your goods and services online, then you will likely be left in the dust in very little time.

Thanks to content management systems and numerous online tools, it has never been easier for even the smallest businesses and firms to create ecommerce stores and to collect data from customers to create more effective marketing campaigns and better-personalized shopping experiences for returning customers. Unfortunately, these new features and online services have come with new potentials for data security breaches.

Those potential risks for your data’s security not only put your business at risk, they also put your customers at risk, as well. This added risk to your customers’ security adds even more liability for your company. When you collect personal or financial information from your customers, you take on the responsibility of keeping that data secure. If you do not operate within industry and legal standards and regulations, you could be held legally responsible for the breach and for any damages that your customers incur from it.

This reason alone should be enough to have you concerned about data security, keeping up with standards and regulations, and ensuring that you are not at risk for a breach. There are, however, a number of reasons to consider data security a top priority for your business.

Fortunately, understanding these and forging a plan to effectively defend your data (and your customers’ data) against attacks is actually fairly simple and straightforward. If you understand how to approach data security, study recent breaches and what went wrong with them, and take a few necessary steps to prevent data theft, then you will be on the road to implementing a solid security strategy and protocol.

What Is Data Security and Why Does It Matter?

Whether you are a small business owner or an executive at a Fortune 500 company, you should have at least some familiarity with cybersecurity and specifically with your company’s data security. Unfortunately, as has been demonstrated by data breach after data breach, all too few executives and boards of directors take the time to understand cybersecurity.

Above all else, if you take nothing else from this whitepaper, you should come away with the understanding that data security is not simply a technological issue that you can allocate to your IT department. No, data security is not just a tech issue – it’s a risk management issue. If you understand and embrace this fact, then you will be one step ahead in the fight to keep your data (and your customers’ data) safe and secure. Essentially, to implement an effective security protocol, you must first think of data security on an intellectual level, not on a technological one. When you consider non-

technological risks for your company, what terms do you use? Most businesses will assess threats and risk levels based four types of risk:

- Reputation
- Business disruption
- Compliance with laws and regulations
- Legal

You can use these metrics to determine the risk associated with a data breach, as well. A large enough breach of the wrong information could potentially affect all four areas of risk for your company. Let's say, for example, that you run an online meal delivery service. Your customers give you their credit card or bank account information, and, in exchange for weekly charges to their accounts, your company prepares and delivers healthy meals and snacks to their doorsteps.

All is well and good with this model until a hacker manages to exploit a security flaw on your website. Suddenly, a large number of your customers' financial information has been breached, and you have to alert your customers that they need to cancel their credit cards and/or contact their banks immediately. How does this situation affect all four or your risk metrics?

- Reputation – When word gets out that you've had a data breach, your customers and potential customers are not going to be too enthusiastic about giving you their financial information again
- Business disruption – All of your customers' whose financial information was breached will now have to cancel their cards and decide whether or not they want to trust you again or cancel services with you altogether. Either way, your business is going to see a major disruption.
- Compliance with laws and regulations – Were you operating within the legal and industry regulations and standards for data security in your field? If not, you could be looking at major problems, both financially and legally.
- Legal – Whether or not you were in compliance with security regulations, you may be open to a number of lawsuits from your disenfranchised customers.

Unfortunately, the only way to ensure that this kind of breach never happens is to avoid collecting customers' data entirely, but if you conduct business online that's simply not a viable solution. Instead, you need to identify the data that presents the greatest potential for threats and risks. Then you must create a risk management and data security strategy that ensures that you have done everything possible to avoid a breach and that complies with all legal and industry data security regulations and standards. Before you move forward to build your digital risk management framework, you should first understand the potential legal ramifications of a breach. If you have truly done everything in your power to prevent a data leak, then you may be able to avoid legal action from your customers, but this is not a guarantee. That's one of the reasons that data security is so incredibly important to businesses today.

Understanding the Legal Ramifications of a Breach

The first and most important thing to understand about the potential legal ramifications of a data breach is that any breach may open you up to the risk of both civil and criminal disciplinary proceedings, as well as fines from regulatory bodies, legal action by any affected partners, and/or lawsuits by your affected customers.

Essentially, avoiding these unpleasant and costly legal actions entails showing that you have done everything in your power to prevent a breach, to minimize data loss in the case of a breach, and to notify your affected customers as swiftly as possible that their data has or may have been breached. This may not prevent some class action lawsuits and other proceedings, but it should minimize your liability and prevent you from being subject to regulatory fines.

Basically, the legal implications and ramifications of losing customer data to hackers come down to two things: tort law and data breach notification laws. The first is tort law, and according to Cornell University Law School, it is defined as the section of laws covering “a wrong which can be redressed by awarding damages.”

In all tort cases, the burden of proof is placed on the claimant to show that the damages they sustained came about out of an act of negligence on the part of the defendant. In other words, if your customers can prove that you acted negligently in regards to their breached information, then they will have a case against you and you will be responsible for paying damages.

Now, whether or not you can prove that you did everything possible to prevent a data breach and avoid damages to your customers, you will still be liable for notifying them about the breach in a timely manner. As of yet there is no national law concerning data breach notifications in the US, but most states and have enacted their own laws covering appropriate legal notification timing and procedures. Likewise, the UK enacted the Data Protection Act in 1998, but it does not specify exact parameters for a company’s legal responsibilities and obligations for notifications.

In the case of a data breach, there is no way to avoid some damage to your company’s reputation, and you will very likely suffer some disruption of business as a result, as well. The key here is to understand that stalling or attempting to hide a breach will in no way help you. The faster you handle the situation and the more transparent you are about how it happened and what you are doing to prevent it from happening in the future, the more trust your customers will retain in you. After the fact, your best damage control strategy is to fix the problem and give your customers every assurance that it will never happen again. This is why a solid data security and risk management plan is essential to the success of any business today. The first step to creating a bulletproof security protocol, though, is to understand the costs that come with data loss.

What Does Data Loss Cost Your Company?

According to Stephen Pritchard, in an article for Computer Weekly, reputation damage is an even larger concern than legal damages. He maintains that stakeholders and customers do not care much whether a breach occurred due to negligence, insider breaches, or a malicious attack by hackers. No matter what the cause of the breach, even if you can prove that it happened through no fault of your business, you can expect to sustain a reputational loss. And, as you know, reputation is everything in the modern

business world.

Pritchard goes on to quote Andrew Jaquith, senior analyst for Forrester Research in Massachusetts, saying, “The side effects of data loss are hard to gauge...There have been several studies on the negative impact on share price for companies that have suffered a breach, but the results have been inconclusive. Certainly, when a company loses control over customer information it has custody of, it also suffers a loss of trust with its customers.” Jaquith also cautions that you are likely to feel this impact more if you’re in an industry in which your customers have low switching costs.

A data breach won’t just affect your reputation and how much your customers are willing to trust you, though. Jaquith points out that a data breach will often invite “scrutiny from business partners, and sometimes result in direct financial losses or reduced business.” To illustrate this, he notes one US financial company that lost its place on the Payment Card Industry’s certified list of payment processors.

Essentially, a data breach can make your business partners and other industry affiliates lose faith in you and want to drop associations with your business. In addition to losing current customers, this can cause major problems for gaining new customers in the future.

You can see, then, just how important data security is and how much your company can benefit from data theft prevention. This, of course, means more than just implementing security measures at random. If you truly want to do everything in your power to prevent the catastrophic consequences of a major data breach, you should understand how to approach the problem, what recent breaches can teach you about data security, and which tools you should use to implement your security strategy.

The Right Approach to Prevent a Data Breach

So how should you approach data security for your company and your customers? Your strategy should follow a fairly simple risk management plan:

Identify sensitive data – What information do you collect from your customers? Start by identifying and locating all potentially sensitive information that you keep, including your company data and data on your customers and employees.

Make sure you’re compliant – If you’re in the healthcare industry in the US, you’re going to be subject to the federal Health Insurance Portability and Accountability Act (HIPAA). Other industries have laws and industry-wide regulations and standards governing them, as well. If you are not in compliance, you are not only opening your company up to a data breach but also to legal action and fines if a breach does occur.

Review your business’ data security policies – If you can’t remember the last time you reviewed and updated your data security policies, then it is past time you did so. This is not only a good practice, but many state and federal laws apply to keeping updated information security policies, so it may be necessary to keep you in good legal standing, too.

Keep access limited – Make sure that employees, vendors, business partners, and others only have access to the data they need to do their jobs. Open access to sensitive data will most definitely increase your risk of being breached.

Don’t just implement digital security measures – Though malicious attacks by hackers far outstrip data lost through physical theft and/or insider breaches, these threats are still quite relevant. Make sure that – in addition to digital measures like firewalls, strong passwords, and encryption – you also have physical security measures in place, as well. These can include paper shredders to dispose of sensitive information, good locks on cabinets and storage rooms, etc.

Ensure that all sensitive data is encrypted – This is especially important for cloud-based data, data stored on mobile devices, and/or transmitted over wireless networks, but it is no less important for the information stored on your servers.

Training is as important as policies – No matter how bulletproof your security policies are, they will not be worth the paper they’re written on if you do not properly train your people and enforce good security practices throughout the company. A hacker won’t need to penetrate your company’s firewall if an employee loses a laptop and neglects to report it. Lost or stolen hardware and other situations like this can leave you open to a breach, but when you implement good practices and training, you’ll have the tools you need to stop a breach before it happens.

Choose your vendors and custodians wisely – Most businesses will not write their own code and develop their own sites for ecommerce and other online transactions. With so many service providers and vendors online today, there’s no need to reinvent the wheel. That said, you should be very careful when choosing vendors, custodians, and other third-party service providers. Make sure that they are in compliance with industry standards and that you can trust them with your customers’ data.

Don’t keep so much data – All too many companies do not realize how much of their customers’ information they store after each transaction. Credit and debit card information may be stored indefinitely with or without customers’ approval, and you may never know until your system is breached. Make sure that you are not collecting and storing unnecessary data and that the data you do collect is done deliberately and with purpose (and that it is properly encrypted).

Get professional penetration testing – While you can do a lot to ensure and maintain the security of your customers’ data, you may be surprised at what you can miss, too. It may befit you to hire a professional information security consultant to perform penetration testing (also called pen testing) to see how easily a hacker could access your company’s (and customers’) sensitive data.

Taking these steps should put you on the right track to avoiding data breaches and keeping your customers’ sensitive information safe and secure. Before you consider which tools you should use to put these processes in place and improve your security, let’s first take a look at a few of the most recent and most devastating breaches across industries.

Recent Branches and What They Mean to You

Understanding what happened with these companies, how the breaches occurred, and what they did to respond to them could help you a great deal in avoiding similar situations in the future for your company.

TalkTalk– Just a few days ago, broadband provider TalkTalk was hit with yet another massive data breach, making this the third data breach for the company in a single year. Not only were millions of customers potentially put at risk, but TalkTalk has also admitted that a large portion of the data was not encrypted. This means that the hackers who carried out the attack may have gained access to thousands of TalkTalk customers' personal and financial information.

The Telegraph has reported that cybersecurity experts find it worrying that TalkTalk has fallen victim to so many attacks in so little time. Essentially, in their eyes, this looks very much like TalkTalk has not taken the situation seriously and has not taken proper measures to update and fortify their security, leaving their customers' data open to anyone with the tools and knowledge to penetrate their system.

Worse yet, some clients have reported that TalkTalk failed to notify them of the breach in a timely manner. In fact, some customers did not learn that their data had been leaked until they found that their bank accounts had been emptied.

One TalkTalk customer who spoke with The Telegraph found out about the breach on the Friday after the attack happened when she checked her account. When she saw that she had lost a large amount of money and that her account was overdrawn, she called her bank to report the problem. "The first question my bank asked me," she told The Telegraph, "was whether I was a TalkTalk customer." TalkTalk had been aware of the breach for almost three full days, but they had failed to notify a customer whose data was clearly leaked. "The first thing I'll do when I get the account running again is cancel my TalkTalk account and find a new broadband provider," and she is not likely to be the only one.

So what can you learn from the fiasco that TalkTalk is now dealing with? Essentially, the broadband provider made two major mistakes with this breach that will cost them greatly. First, they had two previous breaches within the last year and did nothing (or did not do enough) to prevent future attacks from penetrating their system and gaining access to their customers' data. A single breach is an annoyance but is forgivable for most companies. A second breach within a short amount of time of the first one may also be forgiven by customers and business partners if the company shows that it is doing everything in its power to stem the flow of leaked information and stop the problem from occurring again.

However, a third breach, with the revelation that the company has not taken simple security steps like encrypting customers' financial data, looks incredibly bad. This looks very much like TalkTalk took a nonchalant attitude toward its customers' security, which is a great way to lose a lot of business. Second, after the third breach, TalkTalk did not immediately take active steps to notify all of its customers that they were at risk of having their financial information exposed. If customers find out that you have known about a breach for days and have not taken the time to tell them that their bank accounts may be in danger, then they will lose all trust in you and will not want to continue doing business with you.

British Gas - Following hot on the heels of the TalkTalk breach, The Guardian reports that British Gas has notified an estimated 2200 of its customers that their email addresses and British Gas account passwords were briefly published online. While this is the first breach of its kind for British Gas, it's cause for concern for British Gas customers for a number of reasons.

First of all, if an unauthorized person has the email address and password for a customer's British Gas account they may then have access to that customer's bank account or credit card information. They may also be able to lock the customer out of their account by changing the password, as well.

There isn't anything particularly special about the breach itself, but British Gas' response is distressing to a number of customers. According to the BBC, in an email to customers, the company stated, "There has been no breach of our secure data storage systems, so none of your payment data, such as bank account or credit card details, have been at risk. As you'd expect, we encrypt and store this information securely. From our investigation, we are confident that the information which appeared online did not come from

British Gas."

On one hand, this response is at least somewhat comforting. If payment information is encrypted, then customers will not have to be concerned that someone with access to their account passwords could then gain access to their bank accounts and/or credit card information.

At the same time, simply denying liability for leaked account information is not the same as showing true transparency and proving that the leaked data did not come from the company. More details concerning where the attack may have come from and why they are certain that they have not been compromised would promote more trust with their customers.

Vodafone –Vodafone has recently come under fire for the actions of two of its employees two years ago who gained access to the call and text histories on a journalist's phone records. Today, though, Vodafone is in the spotlight not for its employees' breach of someone else's security but because their customers' data has been breached.

Though we have yet to see exactly how Vodafone will handle its employees' behavior and its own responsibility in the case with the journalist, the company does seem to be handling their recent breach in an ethical and transparent manner.

Responding quickly and publicly to the hack, Vodafone announced that data for 1827 customers had been leaked in a criminal attack on Vodafone's network. They also stated that they have launched an investigation to find out where the hackers gained access to Vodafone passwords and email addresses, but they maintain that the Vodafone security protocols were not actually breached.

To put customers' minds at ease, a spokesperson for Vodafone has stated that the limited number of affected customers is evidence of the overall effectiveness of the company's security protocols. Vodafone has also stated that criminals may have accessed those customers' names, mobile phone numbers, and the last four digits of their bank accounts, but that all other information remained secure.

The most important detail concerning how Vodafone has handled this breach, though, is the fact that the company has blocked breached accounts and is assisting those customers in changing their account details to protect them against phishing and fraud attempts.

This shows that Vodafone, unlike TalkTalk, is taking an active role in helping those affected by the breach, maintaining the company's reputation with customers, finding the source of the breach, and preventing something similar from occurring again in the future.

As you can see from each of these examples, there are good and bad ways to handle a breach. If your company falls victim to a data breach, the best thing you can do is to be as active and transparent as possible in notifying your customers and taking all actions possible to fortify your security and prevent future breaches from occurring.

Useful Data Security Tools

Thus far we've talked a lot about the theory of data security and how to approach it, but we haven't gotten very far into the technical aspects of keeping your system secure. To be completely honest, that's

because new security measures and tools are being developed almost every day to combat data loss, theft, and leaks.

The best way to get ahead of the game is not to simply download, install, and implement every recommended tool you see online, but rather to put a good strategy in place that can be easily reviewed and updated to keep your business secure. If you have taken this measure, then you will only need to find the tools that fit your strategy best, rather than feeling as if you're swimming in a sea of security apps, tools, and features. Your strategy will give you the framework you need to assess risk and acceptable risk levels and to choose the proper tools for the job at hand.

As Aaron Agius wrote in an article for Entrepreneur, "Social media can be an extraordinarily effective marketing medium, With that in mind, here are a few of the best data security tools for small and large companies to keep customers' data safe:

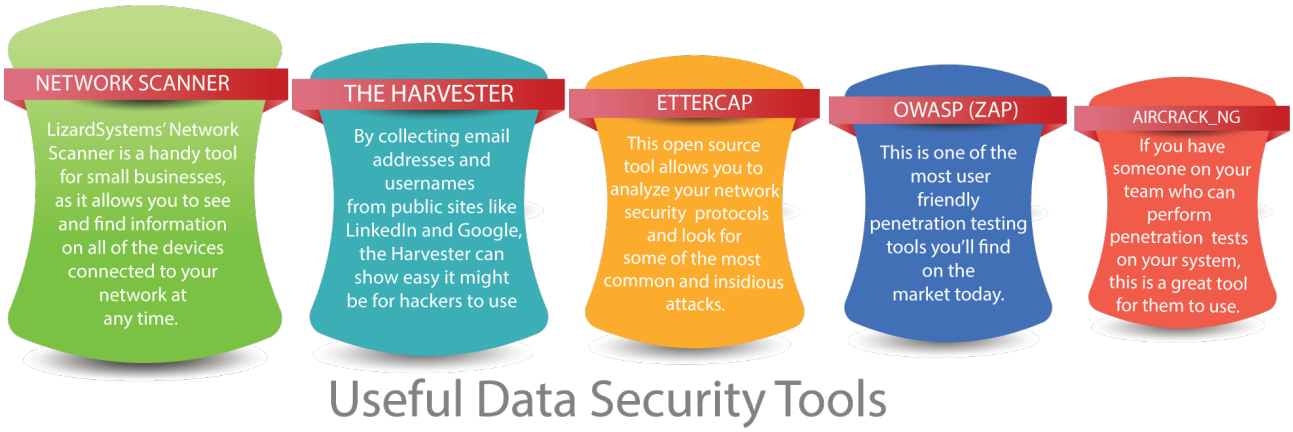
Network Scanner – LizardSystems' Network Scanner is a handy tool for small businesses, as it allows you to see and find information on all of the devices connected to your network at any time. While it scans your network, it will provide you with the IP addresses and other information for all devices using your network, and it will let you know if someone has enabled remote administration, as well. This is a great way to see if someone is attempting to access your network without your permission.

Aircracking – If you have someone on your team who can perform penetration tests on your system, this is a great tool for them to use. It's a comprehensive suite of tools to test your firewalls, encryption, and other potential weaknesses.

Ettercap – This open source tool allows you to analyze your network security protocols and look for some of the most common and insidious attacks. Functionalities include IP, MAC, and ARP-based scanning to give you a full analysis of your network and how secure it is.

OWASP Zed Attack Proxy (ZAP) – This is one of the most user-friendly penetration testing tools you'll find on the market today. With this tool, you can either set scanners to automatically search for vulnerabilities in your network or you can manually test for them.

The Harvester – By collecting email addresses and usernames from public sites like LinkedIn and Google, the Harvester can show easy it might be for hackers to use this publicly shared information to gain access to your network and your customers' data. Want to avoid a situation in which your security protocol seems to be intact but someone has gained access to your network through unknown sources via email addresses and usernames? This is the tool for you.



Get Professional Assistance

Of course, all of these tools may sound like so much Greek to you, and that's just fine. Just like your ecommerce store, your website, and/or your data collection methods, there is no need to re-invent the wheel when it comes to your data security. You do not have to become an overnight security expert to keep your system and your customers' data secure.

In fact, the best way to ensure the security of your data is to identify the sensitive data you collect, assess your risk factors and acceptable risk levels, and then call the information security professionals to consult with you on the best framework, tools, and applications to use for your company.

With these steps in place, you will be better protected against outside attacks, as well as insider threats.

Conclusion

You should understand now that data security is much more a risk management issue than a technological issue. Furthermore, you should understand the legal implications of data loss or theft. If you have a breach, you should know what you are liable for and why, and you should be aware of your responsibilities for notifying your customers as soon as possible, as well.

Data loss can cost your company in multiple ways. It can not only disrupt your business, but it can also severely damage your reputation and open you up to legal action on the parts of your customers, your business partners, and governing bodies, as well. At the very least, if a breach occurs, and it comes to light that you did not do everything in your power to keep your customers' information safe or you did not take the time to notify them about the breach as soon as possible, you will undoubtedly lose business and have trouble gaining new customers. At worst, you could be looking at lawsuits and steep fines.

With the right risk management strategy and framework, you will be able to choose the right tools and/or people for the job of keeping your network safe and your customers' data secure. Whether you have an in-house security team or you choose to work with consultants who specialize in penetration testing and security reinforcement, you will be on your way to maintaining a better system with fewer vulnerabilities.

Of course, if something does happen, you'll need to know how to handle the situation and how to talk to your customers about the breach so that they understand that their security is your top priority. Transparency is key, but you must also know how to communicate the situation to your customers for the

best outcome.

At Peppersack, we are proud to provide our clients with the very best in digital marketing services. From in-depth analytics and content marketing to helping you weather a data breach, we offer a wide range of digital marketing services to meet your needs, no matter how big or small. Contact us today to learn more about how we can help your business grow.

Works Cited:

https://www.law.cornell.edu/wex/tort
http://www.computerweekly.com/feature/Top-seven-data-loss-issues
http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx
http://www.jstor.org/stable/4508530?seq=1#page_scan_tab_contents
http://www.telegraph.co.uk/news/uknews/law-and-order/11949468/TalkTalk-phone-network-hit-by-significant-cyber-attack.html
http://www.bbc.com/news/technology-34663210
http://www.theguardian.com/technology/2015/oct/29/british-gas-denies-responsibility-user-accounts-posted-online-pastebin
http://www.theguardian.com/business/2015/oct/31/vodafone-customers-bank-details-accessed-in-hack-company-says
http://www.pcworld.com/article/224999/10_must_have_utilities_for_small_networks.html
https://www.fcc.gov/cyberforsmallbiz
ttp://www.pcworld.com/article/224999/10_must_have_utilities_for_small_networks.html
http://cloudtweaks.com/2014/03/cloud-security-tools/
http://www.csoonline.com/article/2152794/data-protection/80286-Twenty-free-and-effective-infosec-tools.html
https://www.concise-courses.com/security/top-ten-pentesting-tools/

About Peppersack

Peppersack is a leading digital marketing agency providing SEO and content marketing services that deliver results. Our search engine optimisation services will help to raise your page rank. We deliver proven results in the form of traffic to websites and sales inquiries though integrated inbound marketing campaigns. We make it easy for your potential clients to find you. These services are based on a disciplined approach to research, analysis, business planning and reporting. Support services include content development, social media management and creative design and development.

Contact Peppersack

Please contact us for help and advice with your digital marketing and communications

Email: contact@peppersack.com
Telephone: 0161 926 3670
Atlantic Business Centre
Atlantic Street
Manchester
WA14 5NQ
web: www.peppersack.com