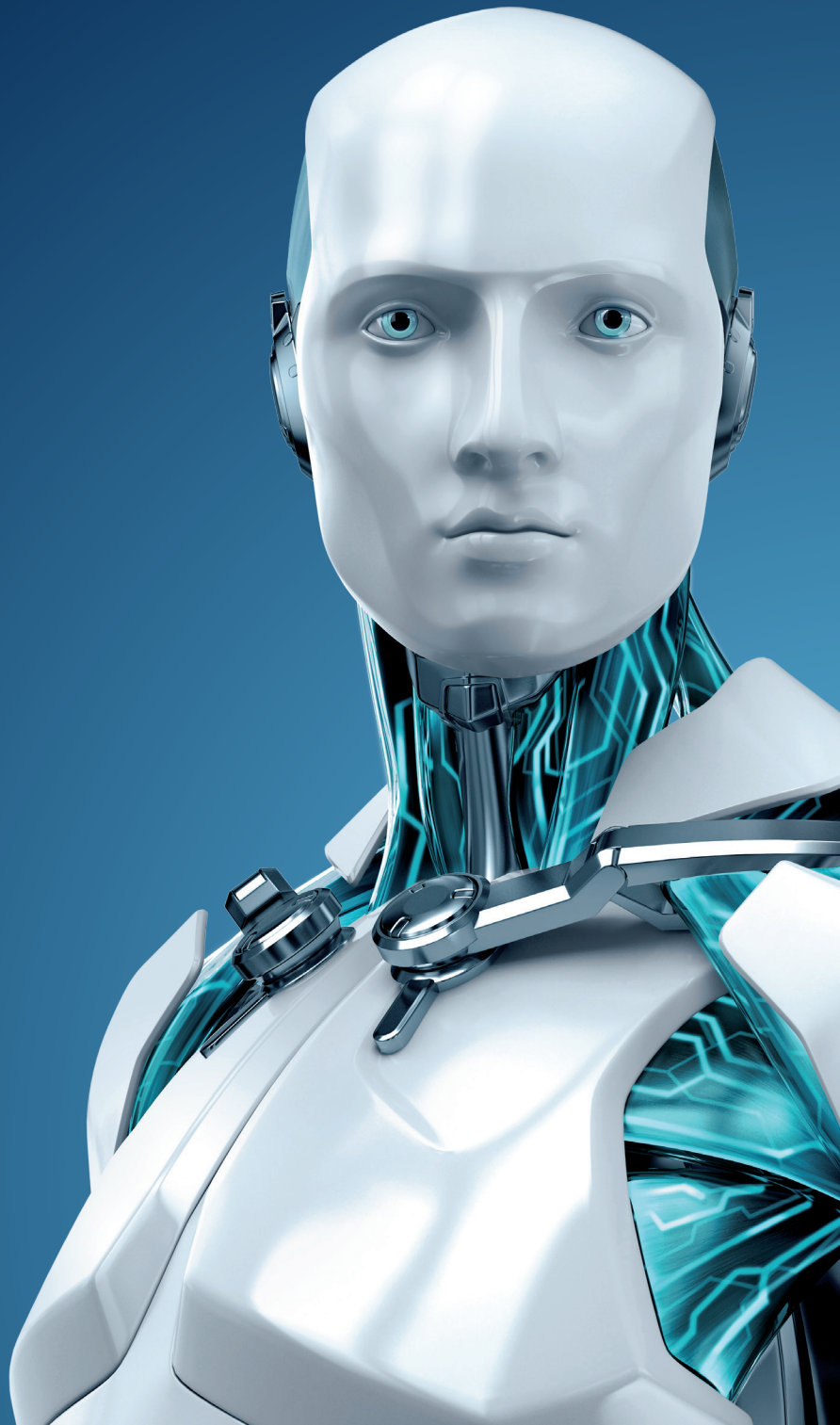
WHITE PAPER

Data breaches, compliance, and the role of two-factor authentication



ENJOY SAFER TECHNOLOGY™

DATA BREACHES, COMPLIANCE, AND THE ROLE OF TWO-FACTOR AUTHENTICATION

By ESET Staff

Abstract

The potential costs of a data breach can shutter a small business, yet many are in denial about the severity of their exposure and necessity to apply diligence in security practices. In the current threat climate, compromised usernames and passwords are often exploited and are one of the leading factors contributing to data loss. Bolstering standard username/password authentication with two-factor authentication guards against lost or stolen passwords and in some cases is a regulatory requirement. Many employees already carry a smartphone that can support two-factor authentication, which makes this security protection practical and affordable for smaller businesses.

Introduction

Regardless of industry and size, every business has the fiduciary responsibility to protect customer data and follow security requirements. While every company is at risk because of the potential loss of customer confidence and the damage to its reputation, the stakes are higher in industries that deal with highly sensitive personal information and are subject to compliance regulations. Therefore, the most vulnerable businesses are those that have personally identifiable information of high value, specifically those in financial services and healthcare, but also those in education and government. Those who have business relationships with such organizations are also at higher risk.

Authentication is one of the fundamental building blocks of computer security. It is the process of verifying a person's identity before granting access to a corporate network or computing resources on that network. The most familiar form of authentication is a combination of a username and password. While there are two separate items involved, this form of authentication, is termed single-factor because both items exercise the same means of verifying an identity—pieces of information that the user knows and remembers. There are other, stronger forms of authentication, such as smartcards and fingerprint readers, that are applied in situations that call for higher security. But for most businesses, single-factor username/password combinations are all that protect the organization from a masquerading intruder and an expensive data breach.

About two-factor authentication. One measure that effectively prevents data breaches—on a number of fronts—is to add another authentication factor. In addition to "something you know"—a username and password—this approach adds "something you have" in the form of a physical item that can be verified independently of the username and password. It is analogous to a physical key or a keycard. The most widely deployed form of two-factor authentication for computer-network access is a computing device or special-purpose piece of hardware that generates a unique "token" (a revolving number) that the user must enter. The device regenerates a fresh token for every login attempt so it cannot be reused, and cryptographic techniques protect against the token being guessed or intercepted. Adding the second factor ensures that even if the username and password have somehow been compromised, a thief

will still not have everything needed to log in and take advantage of system privileges.

In regulated industries that need to comply with statutes such as HIPAA, HITECH, PCI DSS, FFIEC, GLBA, SOX, FACTA, and ADA, two-factor authentication is either a direct requirement or a strongly recommended practice. In particular, when remote workers out of the office log on to the public Internet and access the corporate network, they typically use a VPN connection for security. Here, multifactor authentication is specifically required under most of the regulatory structures for compliance.

Weak authentication and data breaches

A 2012 study that examined 855 data breaches[1] exposed the weaknesses of single-factor authentication for businesses—especially the small businesses that accounted for the great majority of the breaches. Most involved compromised usernames and passwords.

In these incidents, the compromised credentials were only an avenue for gaining access. The actual data theft usually involved installing malware of some kind on the impacted machine. In 48% of incidents, this was a keylogger, form-grabber, or other form of spyware, and in 20%, a remote-access backdoor that gave the intruder control of the machine. In 18% of cases, the malware disabled security controls. In 30%, malware automatically sent stolen data to an external site.[2]

Lost or stolen login credentials are a particular threat, because while they were involved in 32% of breaches, they figured in 82% of the total data records compromised.[3] Gaining full user access to the network through valid credentials is like walking through an open door; the intruder can simply help himself to whatever files and data he can find. This is how mass compromises occur. In one case, 50 million usernames, email addresses, encrypted passwords, and, in some cases, dates of birth were stolen due to a hacker intrusion.[4] In another incident, a company that ironically is in the business of helping customers keep their private data off of the Internet was itself breached, resulting in the exposure of names, email and physical addresses, and, in some cases, phone numbers, dates of birth, and occupational information. The exact number of individuals affected was not disclosed.[5]

BREACHES WHERE IMPLICATED (%)	ATTACK VECTOR	DESCRIPTION
44%	Weak credentials	Usernames and passwords left at default or easily guessed, such as admin, user, password
32%	Lost or stolen credentials	Usernames and passwords compromised by lost or stolen devices, installation of keylogger software that detects passwords, or stolen data that contained login information
23%	Brute force or dictionary attacks	Automated login attempts that try large numbers of usernames or passwords until one works
5%	Insufficient authentication	Exploits that take advantage of lax authentication procedures, such as logins not required, or that allow "blank" passwords

Table 3: Numbers add up to more than 100% because some compromises involved multiple causes; e.g., a weak password guessed by a simple dictionary attack.

1 Verizon RISK Team. 2012 Data Breach Investigations Report, 2012.

2 Verizon RISK Team. 2012 Data Breach Investigations Report, 2012.

3 Verizon RISK Team. 2012 Data Breach Investigations Report, 2012.

4 LivingSocial Hack Exposes Data for 50 Million Customers, The New York Times, April 26, 2013. http://bits.blogs.nytimes.com/2013/04/26/living-social-hack-exposes-data-for-50-million-customers/

Breaking the data breach cycle

Two-factor authentication is becoming increasingly important as personal lives and technological lives become intertwined. With so much personal interaction and financial business being done online, with shared account names and passwords and sharing of credentials, one account breach can lead to another, and then another. In one such case, daisy-chained accounts led to a technology journalist's entire digital life being compromised across Google, Twitter, and Amazon. The attackers performed a remote wipe of his iPhone®, iPad®, and MacBook® not out of malice, but to impair his ability to regain control of his accounts. He stated that using two-factor authentication would have broken the chain that allowed the multiple compromises.[1]

In another case, the inherent dangers of public cloud services relying only on username/password authentication were highlighted. Usernames and passwords stolen from various sites were applied to access accounts at a cloud services provider, leading to theft of user emails stored in one employee's account, in turn leading to those users receiving spam promoting gambling sites. In response, one item of corrective action was that the cloud services company announced it would begin requiring two-factor authentication.[2]

The latter case summarizes the perils of a business getting caught in a cycle of data breaches—even if the business was not involved in the initial breach. Users often reuse their names and passwords on multiple sites and rarely change them. When stolen, often through mass compromises, they then serve as the key to accessing the user's accounts with other sites and services. Stolen data is readily available and inexpensive, and there is even an underground online black market for such personal information.[3] In the current environment, the simple combination of username and password is no longer enough.

The financial impact of stolen data

Failure to protect data can result in litigation, fines, and more. Recent security incidents show that authorities are willing to enact severe penalties on organizations that fail to take prudent measures to protect private data in their possession. Some of the more prominent examples:

Wyndham® Hotels. The world's largest hotel company was sued by the Federal Trade Commission for three data breaches in less than two years. Lack of basic security measures allowed access to more than 600 credit card accounts, resulting in $10.6 million in fraudulent charges.[4]

Sony®. A staggering 100 million accounts compromised among various online properties resulted in more than 25 lawsuits, including a class action alleging negligence, breach of contract, and consumer privacy violations.

The stakes are becoming ever higher. A recent high-profile Associated Press social media hack by the Syrian Electronic Army

1 Mat Honan. How Apple and Amazon Security Flaws Led to My Epic Hacking, August 6, 2012. http://www.wired.com/gadgetlab/2012/08/apple-amazon-mat-honan-hacking/all/

2 Dropbox Password Breach Highlights Cloud Security Weaknesses, ZDNET, August 3, 2012. http://www.eweek.com/c/a/Security/Dropbox-Password-Breach-Highlights-Cloud-Security-Weaknesses-266215/

3 Kashmir Hill and Zack O'Malley Greenburg. The Black Market Price of Your Personal Info, Forbes, November 29, 2010. http://www.forbes.com/2010/11/29/black-market-price-of-your-info-personal-finance.html

4 FTC Sues Wyndham Hotels over Data Breaches, CNET, June 26, 2012. http://news.cnet.com/8301-1009_3-57460551-83/ftc-sues-wyndham-hotels-over-data-breaches/

and corresponding tweets about explosions at the White House had immediate repercussions in the financial market to the tune of a $136 billion fluctuation.[5]

Risk to small businesses

The 2012 study of 855 data breaches found that most cyberthieves are professional criminals looking to steal data that they can turn into financial gain. Larger organizations are more likely to be targeted to gain access to trade secrets and organizational data. By contrast, smaller companies are more likely to be targeted for personal information, including bank account and credit card numbers, medical records and other classified information, and authentication credentials, which could be used as tools for further compromises. More than 75% of the breaches occurred at organizations with fewer than 1,000 employees.[6]

Why so much focus on smaller organizations? It is part of a long-term trend that security experts have noted, as larger enterprises invest in security measures and harden their defenses, causing the organized criminals to look for easier prey.[7] Smaller organizations do not have the same resources to invest in security, yet provide tempting targets for harvesting personal information and, once breached, can also serve as avenues for penetrating larger partners.

Despite the statistics, many small businesses are in denial. A study from the Ponemon Institute that polled 1,200 U.S. businesses with less than $10 million in annual revenue found that only 33% of businesses that had experienced a data breach informed the breach victims, despite laws in 46 states requiring notification.[8] The same study found that:

- 55% of businesses surveyed reported at least one data breach
- More than 50% reported being compromised multiple times
- 9% said they lost count of how many times breaches occurred
- 8% lost personally identifiable information (Social Security, driver's license, and credit card numbers)

And they are in denial about the risk, based on the Hartford Small Business Data Protection Survey:[9]

- 85% believe a data breach is unlikely, and many are not implementing simple security measures to help protect their customer or employee data
- About a third of business owners (34%) say they would have difficulty complying with government notification requirements

5 Syrian Hackers Claim AP Hack That Tipped Stock Market by $136 Billion. Is It Terrorism?, Washington Post, April 23, 2013. http://www.washingtonpost.com/blogs/worldviews/wp/2013/04/23/syrian-hackers-claim-ap-hack-that-tipped-stock-market-by-136-billion-is-it-terrorism/

6 Verizon RISK Team. 2012 Data Breach Investigations Report, 2012.

7 Parija kavilanz. Cybercrime's Easiest Prey: Small Businesses, CNN|Money, April 23, 2013. http://money.cnn.com/2013/04/22/smallbusiness/small-business-cybercrime/index.html

8 HSB Survey Finds Half of Small Businesses Had a Data Breach, HSB, February 2013. http://www.hsbwhistlestop.com/agents/express/2013/02/hsbSurvey.php

9 Small Business Owners—Despite Being Increasingly Targeted—Believe Data Breach Unlikely, June 6, 2012. http://newsroom.thehartford.com/News-Releases/Small-Business-Owners-mdash-Despite-Being-Increasingly-Targeted-mdash-Believe-Data-Breach-Unlikely-50c.aspx#downloads

Sizing up the total risk

According to a report from Zurich General Insurance,[15] the costs of dealing with and remediating a data breach have the potential to bury a small business. The bigger the breach, the larger the costs, both direct and indirect.

Fines and penalties. The most direct financial risk is the failure to comply with standards and being fined as a consequence. For example, PCI DSS requires that companies enact a broad array of safeguards for personal credit card data, with the possibility of fines, expensive remediation, or both for businesses that fail to comply with one or more of the requirements. In addition, 39 states have enacted their own regulations for failure to protect sensitive personal information. In one case, a Massachusetts restaurant group was fined $110,000 for failing to comply with PCI DSS and other standards.[10] In another case, a small-business data breach in Idaho resulted in a $50,000 fine under HIPAA for failing to protect confidential patient data.[11]

Forensic Examination	$174 - $268 / Record
Notification of Third Parties	$.50 - $5 / Record
Call Centers	Varies
Credit Monitoring	$10 - $30 / Record
Reissue of Payment Cards	$12 - $22 / Card
Public Relations	$214 / Record
Legal Defense	$500K - $1M / Record
Regulatory Fines and Penalties	$5K - $100K / Month

Remediation costs. PCI DSS requires that companies that store or process credit card data implement strong access control measures,[12] and those that have not used readily available security measures have been involved in large settlements that required extensive and expensive remediation.[13] Smaller businesses might find themselves having to undergo audits, or be made to comply with the more expensive and stringent requirements that are mandated for larger enterprises.[14] In addition, the various regulations require that the business notify the individuals whose personal data has been compromised, and in some cases it might be required to pay some restitution costs depending on the nature of the breach. Since standard business insurance policies do not cover the costs of a data breach,[15] a fine and subsequent remediation of a large breach could shutter a small business.

Reputation and goodwill. Knowing that a business has been lax in securing personal data makes customers think twice about engaging with that business. Likewise, potential partner businesses want to

10 Massachusetts Enforces Controversial Data Security Program: $110,000 Penalty for Lax Data Security Practices, April 1, 2011. http://www.fr.com/data-security-program/

11 Small Business Data Breach Triggers $50K Fine, January 8, 2013. http://www.techinsurance.com/blog/cyber-liability/small-business-data-breach-triggers-50k-fine/

12 PCI Security Standards Council, PCI DSS Quick Reference Guide: Understanding the Payment Card Industry Data Security Standard Version 2.0, October 2010, p. 18.

13 Federal Trade Commission, Agency Announces Settlement of Separate Actions Against Retailer TJX and Data Brokers Reed Elsevier and Seisint for Failing to Provide Adequate Security for Consumers' Data, March 27, 2008. http://www.ftc.gov/opa/2008/03/datasec.shtm

14 Merchant PCI DDS Compliance & What Is PCI Compliance? http://usa.visa.com/merchants/risk_management/cisp_merchants.html#anchor_2

15 Data Breach Liability and Protection. https://www.zanderins.com/data/data_breach.aspx

know that those they do business with have solid security practices in place to protect their own liability.

If two-factor authentication solves many of the vulnerabilities of username/password-only schemes, why don't businesses adopt it more widely? The answer is, the pain of change. If the business abruptly decides to require two-factor authentication, how many employees have the device necessary to meet the requirement, how will IT support them, and how much employee dissatisfaction will it cause? Many companies choose instead to make two-factor authentication optional, but since it's not a requirement, users are reluctant to opt in. A deployment entirely funded by the business is often out of reach for a smaller organization, especially when the need is weighed against the available or projected budget.

Advantages of software two-factor authentication

Two-factor authentication is standard practice for large enterprises that want secure mobile access for their workers in the field. Historically, most systems have used a hardware USB dongle that generates the onetime token/password. Unfortunately, these hardware-dependent systems are difficult and expensive for small businesses to implement.

Software solutions take advantage of a hardware device that users already have—typically a smartphone—which makes them much more affordable and practical for small businesses that need to meet the standards for compliance. One such solution from ESET® can be added onto existing security infrastructure, with minimal deployment required, and can integrate with Microsoft Management Console and Active Directory. It supports most smartphone platforms, using a mobile application to generate and deliver the token, as well as legacy J2ME devices that deliver tokens via SMS text messages.

Such a solution simply and affordably corrects for the vulnerabilities of single-factor authentication:

Weak passwords—Even if the user doesn't follow guidelines by maintaining (and regularly changing) a strong password that is not easily guessed and thwarts dictionary attacks, requiring the second factor still throws up a roadblock that protects the computer, network, and business.

Mass data breaches—If authorization credentials are lost in a mass data breach or by a third party, enforcing two-factor authorization on all logins means that the token-generating smartphone or physical factor—"something the user has"—is also required to make use of the stolen information.

Lost or stolen laptops—If a laptop is lost or stolen and the usernames and passwords are automatically saved in the settings, the second authentication factor is still needed for access to the business network.

Part of an overall security strategy

Two-factor authentication is part of an overall security strategy.[16] No single system or technology will prevent all attacks; therefore, security and protecting data are ultimately the responsibility of the business. Paying due diligence to relatively simple actions and precautions now is better than dealing with the consequences of a

16 Susan Payton. Only You Can Prevent a Data Breach, Small Business Trends, November 1, 2011. http://smallbiztrends.com/2011/11/only-you-can-prevent-a-data-breach.html

breach later, and employee education is a key piece of any prevention strategy. Clicking on malware-laden emails remains one of the most common ways of infiltrating a network. Attacks that trick properly authenticated individuals into performing unsafe actions, such as clicking on, executing, and installing files of unsafe origin, can't be stopped by extra layers of authentication. "Spear-phishing" attacks are aimed at known individuals and prey on familiarity, curiosity, and clever social engineering to goad recipients into compromising their own machines. One such email attack targeted specific individuals at the *New York Times*, and led to installation of Chinese malware that compromised the systems of 53 employees, mostly remote workers. All *New York Times* employee data was subsequently exposed as a result.[17]

Therefore, two-factor authentication needs to be implemented as one component of a multilayered solution that encompasses endpoint protection, including antivirus and antispyware, server, and mail-security solutions. The security strategy needs to be regularly reviewed and improved as cybercriminals become more clever and determined to find new angles to exploit.

Conclusion

Small businesses—especially those in regulated and vulnerable industries—need to pay just as much attention to security issues as larger enterprises. This is not just for the protection of their customers, but for the protection of the business. Implementing two-factor authentication adds a vital extra layer of defense that effectively protects the business against compromised usernames and passwords. Adding this extra protection by using employee smartphones as the "second factor" makes this extra protection practical and affordable for smaller businesses.

17 Catherine Shu. The New York Times Was Attacked by Chinese Hackers over Four Months, TechCrunch, January 30, 2013. http://techcrunch.com/2013/01/30/the-new-york-times-was-attacked-by-chinese-hackers-over-four-months/