CROSSMATCH®

The world identifies with us.℠

WHITE PAPER

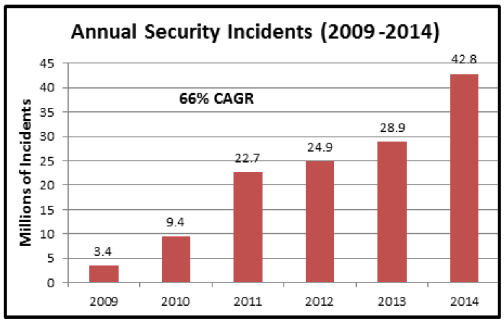
DATA BREACHES
AUTHENTICATION METHODS MATTER

Data Breaches - A Present and Growing Threat

2014 was marked by continued cyber attacks affecting companies and organizations of all sizes in all industries. The 2015 Data Breach Incident Report published by Verizon reported 2,122 confirmed data breaches in 61 countries affecting all industry and government sectors. Cyber crime is huge and pervasive. No one is immune and no one has been left untouched.

More than 2100 confirmed data breaches in 61 countries in 2014.

Given the number and severity of the breaches reported over the past year, it comes as no surprise that security incidents are growing at an astounding year-over-year rate. Reported security events have increased over the period of 2009 to 2014 at a CAGR of 66%. As indicated in the chart, the total number of security incidents climbed to 42.8 million in 2014 alone, an increase of 48% over 2013. That's the equivalent of 117,339 incoming attacks each and every day. This only takes into consideration incidents detected and reported. Many incidents remain undetected or go unreported. We are left with the troubling reality that the number of cyber attacks continue to increase and show no sign of abating.

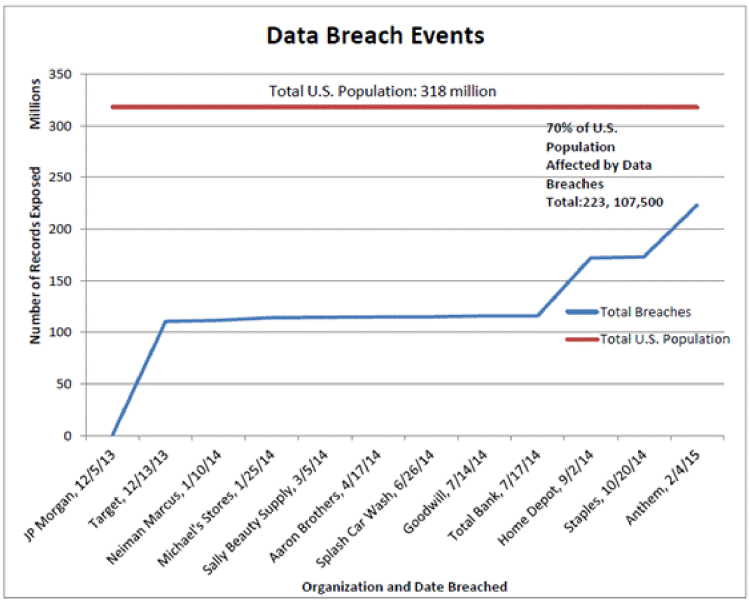


The Global State of Information Security Survey 2015 - PwC

It's Not Just the Number of Breaches

Although the number of data breaches show an alarming rate of growth, more troubling is the sheer number of records stolen in these breaches, jumping a whopping 78%, from 575 million in 2013 to more than one billion in 2014.[1]

To put the scale of this theft in perspective, the chart below shows that from November 2013 to February 2015, a full 70% of the U.S. population became victims of data breaches.

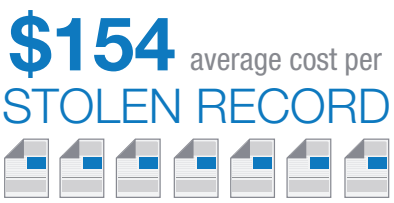


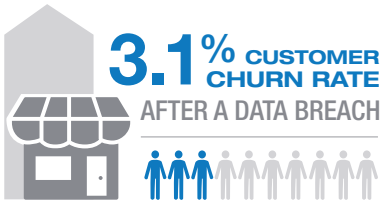
Copper River Group: Data Breach Events and the U.S. Population Report

Financial Impact of a Data Breach

In 2014, the average cost of a data breach was $5.2 million.[2]

Financial costs continued their relentless march upward during the past year. A sampling of key findings from the Ponemon 2015 Cost of Data Breach Study paints an alarming story:





The probability of a data breach involving a minimum of 10,000 records is estimated at 22%. Though no company is exempt, retailers, financial services and healthcare have amongst the highest estimated probability because of the amount of confidential and sensitive information they collect.

The costs associated with a data breach can range from painful to ruinous. According to a study cited by the U.S. House Small Business Subcommittee on Health and Technology, nearly 60 percent of small businesses will close within six months after a cyber attack. The tragedy is that many breaches can be stopped in their tracks by adopting basic security precautions, as we will see.

Best Practices to Reduce Data Breach Risks

The sheer number and destructiveness of data breaches in the past few years are alarming and discouraging. However, there is cause for hope. Most of the cyber attacks had a great deal in common. One of the most compelling similarities in all attacks was the use of compromised credentials. Three-quarters of all breaches were largely due to weak or stolen credentials.[3]

The good news is that the vast majority of security breaches can be prevented by implementing and enforcing basic security best practices. Best practice recommendations for preventing security breaches come from every corner of the industry, analysts, consultants, governmental bodies and security organizations alike, and they speak as if with one voice.

Create and Enforce Strong Password Policies

- Require strong passwords consisting of a minimum of 8-characters incorporating alphanumeric and special characters.
- Force password changes every 90 days with no reuse.
- Avoid storing passwords unless absolutely necessary. If storing passwords, make sure that they are encrypted.
- Do not cache administrative credentials. An explicit login should be required for each session, on all critical systems.
- Do not use factory default usernames and passwords for local or remote access to systems.
- Assign strong, unique passwords to third party vendors. Do not use these same passwords for internal systems. Do not use the same credentials for multiple vendors.
- Delete all default and inactive accounts from all devices and perform regular audits for such accounts.
- Immediately delete accounts for terminated employees or third parties.

Employ Multi-Factor Authentication

- Single-factor, password-based authentication simply isn't good enough anymore. Use multi-factor authentication to make it very difficult to steal or reuse credentials for fraudulent purposes. This is a must for administrative accounts, third-party vendors and service providers.
- All remote access and critical internal services and machines, such as Domain Servers, should be protected by requiring multi-factor authentication.
- Monitor these accounts frequently to detect unusual activity.

Restrict Remote Access

- Limit remote access by third-party vendors and service providers.
- Create and enforce security policies governing remote access.
- Monitor remote access sessions for aberrations, such as frequent failed login attempts, logins outside of standard business hours and extended duration.
- Lock out accounts after multiple failed login attempts.

Following these recommended industry best practices would have prevented a lion's share of the breaches in the past few years. One can hope that the very real threat of attack and the gruesome fallout afterwards will motivate companies to adopt these basic recommendations. However, to adopt a more parochial view, you don't have to outrun the bear, just your companion. Hackers are opportunistic and look for an easy mark. With a few precautions, you can send the criminals searching for easier pickings.

Limitations of Existing Authentication Methods

Tokens and cards can be stolen, lost or shared.

The vast majority of devices and applications only require a username and password for entry, but as we have seen, passwords can be stolen or easily guessed. Although strong password management policies can make it harder for hackers to crack passwords, getting users to abide by stringent password policies has largely failed because of basic human factors. Passwords are cumbersome to enter and remembering strong passwords, especially if they are regularly rotated, are beyond the ability of most users. Instead, they are written down on yellow stickies and attached to monitors or entered as plain text into PC files, readily available for cyber criminals to steal.

The use of tokens and cards also comes with inherent limitations; they can be stolen, shared, or lost and are expensive to provision and maintain. They also are cumbersome to use, interrupting normal user workflow and reducing productivity.

One of the key weaknesses of these existing authentication methods is the lack of identity awareness. Authentication credentials, such as passwords, PINs, tokens or cards, do not guarantee the identity of the person using them. Thus, they provide no accountability and can be refuted.

Enter Biometrics

As a second or third factor, biometrics afford unique and powerful security safeguards not possible with other authentication credentials.

Proof of Presence
The use of fingerprint biometrics requires that the person whose identity is bound to their biometric must be present at the time of authentication. Not only do biometrics provide strong authentication, but also supply irrefutable proof of who did what and when, making people accountable for their actions.

Ease of Use
Fingerprint biometrics are inherently easy to use. Touching a fingerprint sensor is a natural interface, as easy and intuitive to use as pushing an enter key. Because there is nothing to remember or manually enter, using a fingerprint sensor is quick and doesn't interrupt workflow.

Security Integrity
Fingerprint biometrics cannot be lost, stolen or shared. They are a potent antidote to data breaches, most of which depend on compromised credentials to access corporate systems and data. Ultimately, strong biometric authentication lowers the risk to the organization and is a significant deterrent to hacking or the misuse of privileges.

Reduce Costs
Users are freed from having to remember complex passwords eliminating costly help desk interventions to reset passwords.

Crossmatch® Security Solutions

Multi-factor authentication with biometrics offers stronger security and proof of presence.

Crossmatch has the identity solutions you need to empower your workforce and protect the physical and digital assets that are important to you. Employees and other authorized users simply must have anywhere-anytime access to secure networks and databases in order to get their jobs done. The proliferation of cloud-based applications, mobile technology and BYOD cultures makes this a challenge for organizations of all sizes.

Crossmatch delivers the industry's widest range of proven authentication and access management solutions for securing access to your applications, computers and networks. Our multi-factor approach, which incorporates the unmatched certainty of biometrics, has been adopted by leading organizations worldwide in a variety of industries. Financial institutions, retailers and a long list of defense, government and law enforcement agencies deploy our biometrics-based solutions to meet their identity management challenges.

DigitalPersona® Altus

DigitalPersona Altus provides a centrally-managed, strong authentication client and server. Altus leverages multiple authentication credentials, including fingerprint biometrics, smart cards, Bluetooth and other secure, yet affordable technologies. Additional authentication clients on Android or Linux can be developed and connected to the Altus infrastructure using REST compliant Web Services or Android Authentication Layer. The solution enables you to create assured identities and subsequently authenticate employees, customers and partners in real-time anywhere.

TO LEARN MORE

For more information, visit www.crossmatch.com or contact us at:

- In North America, call: +1 561 622 1650
- In EMEA, call: +44 1189 654001
- In Asia, call: +886 2 2735 5586

Key Benefits of DigitalPersona Altus

- *Biometrics Support*. Bind authorized user identities to their biometrics for strong authentication.
- *Configured to your policies*. User identity management, remote authentication and access privileges are managed according to your specific business rules.
- *Successful deployments*. Program success is enhanced with Crossmatch consulting services, which include options for assessment, design, deployment and support.
- *Low administration costs*. Altus integrates with existing Active Directory infrastructure and is easy to use and maintain. Administrators can monitor activity and update, enhance or revoke privileges.
- *Flexible and scalable*. Altus is designed to scale to meet increased demand and can grow with your user base.
- *Trusted by industry experts*. Dell, HP and other industry leaders integrate Crossmatch biometrics-based solutions as a core security and access technology.
- *Reporting feature*. Assists with compliance mandates (i.e. record of user access to computers and applications).

About Crossmatch

Crossmatch helps organizations solve their identity management challenges through biometrics. Our enrollment and authentication solutions are trusted to create, validate and manage identities for a wide range of government, law enforcement, financial institution, retail and commercial applications. Our solutions are designed using proven biometric technologies, flexible enrollment and strong multi-factor authentication software, and deep industry expertise. We offer an experienced professional services capability to assess, design, implement and optimize our identity management solutions for a customer's individual challenges. Our products and solutions are utilized by over 200 million people in more than 80 countries.

Learn more at www.crossmatch.com

REFERENCES
1. 2014 Breach Level Index
2. Verizon 2015 Data Breach Investigation Report
3. Verizon 2014 Data Breach Investigation Report

Crossmatch
3950 RCA Boulevard
Suite 5001
Palm Beach Gardens, FL
33410
USA
Tel: +1 561 622 1650
Fax: +1 561 622 9938
www.crossmatch.com

CROSSMATCH®