WHY PASSWORDS AREN’T STRONG ENOUGH
Making the Case for Strong Authentication

The risks associated with the use of password-only authentication are not new. In 1995, the US Computer Emergency Response Team (CERT) reported that approximately 80 percent of the security incidents they received were related to poorly chosen passwords. More than fifteen years later, two-thirds of organizations are still using just a password to secure remote access1.

With today’s threat landscape and the increased value placed on the information created and stored, systems that rely on static passwords for security are left vulnerable and at risk of being breached. In this paper, we will examine the need for strong authentication and explore the return on investment that can be realized in order to help organizations make an informed decision when contemplating their strategic move toward more effective security.

The Need for Strong Authentication

Today’s organizations face an advanced threat landscape and a complex regulatory environment that can impede their business objectives directly. Therefore, protecting access to information and assuring the identities of users requesting that access are core elements of any security initiative.

But cybercriminals have begun to recognize the value of enterprise credentials and proprietary information, and as threats such as phishing and malware continue to evolve, they are becoming more challenging to contain. Despite the fact that “password-only” authentication is recognized for providing relatively weak security, the use of a single password as a means of assuring user identities continues to dominate. A primary “weak link” is the employee, who may engage in poor password management practices and work around established security policies to make his job easier.

In the last few years, numerous industry regulations have been issued that require organizations to enact strong authentication security measures to protect against unauthorized access to information. Today, as functionality and technology move to new channels, so do the myriad of threats thus driving an increasing demand for strong authentication across the organization.

---

1 RSA 2011 Workplace Security Survey
– **The online and mobile channels**. Organizations continue to recognize the opportunities and cost efficiencies associated with providing real-time access to information online. As a result, an increasing number of Web-based customer portals and business applications are being launched that enable customers to access and manage their accounts 24/7. Mobile access – smart phones in particular – provides customers with similar access and offers even more functionality through customized applications.

– **Remote and mobile access**. The global nature of business and employee mobility has forced many organizations to provide employees and other end users around-the-clock access to corporate email and other business applications from multiple locations and multiple devices – including smart phones.

– **Access for new user populations**. Today’s organizations are extending access privileges beyond the employee to external contractors, partners, and suppliers to facilitate and streamline business processes. These new user populations require on-demand access to proprietary information such as sales forecasts, competitive intelligence, pricing charts, inventory, and customer data.

**Inside the Threat Landscape**

As organizations extend information – and access – to new channels, the risk of unauthorized access or being targeted by a cyber attack increases. Perhaps the most inhibiting factor preventing many organizations from fully utilizing and realizing the potential of a new channel is security – or, more accurately, a lack of effective security. Ultimately, business objectives and the benefits of the new channels may win out. The potential for increased business opportunities, new revenue streams, and improved customer satisfaction and loyalty drive organizations not only to make the move to the new channels – but also to apply strong authentication to protect access to their network and their valuable business data against the growing number of threats on both sides of the firewall.

**Internal Threats**

Employees use multiple systems, devices, and applications that require separate and disparate log-ins and passwords. This often leads to unsafe password practices such as using the same password on multiple systems, sharing passwords and keeping a record of passwords in handwritten or electronic documents. Among business professionals surveyed on password management, 41 percent of employees stated they have used the same password to access multiple accounts and 25 percent admitted to writing their passwords down on paper in order to remember them². Poor password management practices are putting organizations at risk every day.

The growth of the mobile workforce and anytime, anywhere access from multiple devices are other examples of the threat posed by insiders. Today, the range of end user devices being used for access is growing; 47 percent of employees regularly access their corporate network or webmail through a mobile device such as a BlackBerry or iPhone³. The use of public computers, kiosks, and wireless hot spots is also a common practice for accessing corporate systems, creating an opportunity for a key logger and other malicious programs to steal employee passwords.

**External Threats**

Using methods such as advanced social engineering, phishing scams, Trojans and other forms of malware, hackers target any and all access paths to the corporate network – including SSL VPN and mobile user credentials. The goal? To gain insider access to corporate networks and steal valuable company-sensitive information such as intellectual property, personally identifiable information (PII), corporate data, and trade secrets.

---

² RSA 2011 Workplace Security Survey
Botnets, in particular, present a serious threat to organizations as most infections come with a malware program designed specifically to infiltrate corporate networks and perform specific tasks that siphon out sensitive information or steal passwords. Today, botnet activity can be accounted for in nearly 90 percent of the Fortune 500 organizations\(^3\). Because small and mid-sized businesses are capable of spending only a fraction of what their enterprise counterparts do on security technology, this segment is particularly vulnerable to cyber threats.

Another form of external threat targeting organizations is spear phishing, a form of phishing attack that is targeted mainly at employees or high-profile targets in a business. Spear phishing emails attempt to get a user to divulge personal or sensitive information or click on a link or attachment that contains malicious software. Once the user clicks on the link or attachment, malware is installed, usually in the form of a key logger. With this method, the hacker is able to capture and steal anything the user types, including corporate credentials, bank account information or other sensitive passwords.

Most government regulations call for the use of strong authentication to protect access to applications and systems that contain sensitive data.

### The True Costs of Password Authentication

For many organizations, IT budgets are limited, and cost often is the biggest hurdle to overcome in making the case for strong authentication. In fact, cost is exactly why the use of passwords persists as a security “solution” – the acquisition costs of password authentication are near zero. However, this authentication method – once viewed as “free” – is expensive in terms of ongoing management and support costs. According to the Help Desk Institute, roughly 30 percent of all help desk calls are for password resets – and cost between $25 to $50 per call. This “unseen” cost can be taxing on IT resources and does not account for the impact of lost productivity for the end user.

Compliance is another consideration when determining the true costs of password authentication. Many government and industry regulations require the use of strong authentication in order to meet compliance. By failing to provide additional protection beyond a static password for users accessing sensitive data, organizations may be subject to hundreds of thousands of dollars in regulatory fines and penalties.

Overall, passwords are weak and compromised easily, which puts organizations at high risk for a data breach. The average cost to a business for a data breach in 2010 was $7.2 million, or $214 per compromised record\(^4\), which factors in numerous costs such as customer notification, forensics and investigation, legal fees and potential fines. Then there are the intangible costs, such as the impact of a breach on customer trust and loyalty as well as damage to the business’ brand and reputation.

### Cyber Threats Have No Boundaries

The distribution of malware has extended beyond the financial industry and increasingly is affecting businesses in other industries as well, including healthcare, insurance, telecommunications and education as well as government agencies. The original intended goal for most cybercriminals was to infect online users with a Trojan to collect their bank account information or credit card numbers. By extending their reach into new industries, criminals are targeting a new set of valuable information that can be resold, including patient medical records, personally identifiable information (PII), proprietary corporate data, and sensitive government information that can compromise the security of entire countries.

---

\(^3\) RSA white paper, “Malware and the Enterprise: Understanding the Potential Impact of a Trojan Infection,” May 2010

\(^4\) Ponemon Institute, “2010 U.S. Cost of a Data Breach”
Consumers are also employees, and employees conduct personal business and check personal email accounts from corporate workstations. Similarly, as organizations extend their information and access to new channels and make access available to a wider array of resources, the variety of devices touching the corporate network expands to include “uncontrolled” consumer devices such as the family computer, smart phones, PDAs and iPads. These devices, which may not have any security measures in place, put the organization at higher risk for malware infections and data loss.

Volumes of business data are landing in the hands of cybercriminals, usually unbeknownst to the organization. To demonstrate, after nearly three years of work tracking the Sinowal Trojan, RSA discovered that the data in the possession of cybercriminals extended beyond bank accounts and credit and debit cards; it also included email addresses and passwords and FTP and VPN login credentials. This discovery was one of the first of many that demonstrated just how vulnerable the sensitive data of organizations and government agencies is to the threat of increasingly persistent and malicious adversaries.

An Overview of Strong Authentication

The key difference between password-based authentication and strong authentication is that the user must provide more than one factor, or proof, in order for a successful authentication to be made.

In deciding on the type of strong authentication to deploy, organizations can choose from a range of solutions and form factors available on the market today. Each solution and form factor offers different value propositions in terms of security, portability, scalability, ease of use and end user convenience, reliability and, of course, total cost of ownership.

One-time password authentication

One-time password (OTP) authentication is one of the most popular strong authentication methods being used today for protecting access to corporate networks. Often referred to as two-factor authentication, it is based on something you know (a PIN or password) and something you have (an authenticator). The authenticator generates a new random code every 60 seconds, making it difficult for anyone other than the genuine user to input the correct code at any given time.

To access information or resources protected by one-time password technology, users simply combine their secret personal identification number (PIN) with the code that appears on their authenticator display at that given time. The result is a unique, one-time password that is used to positively assure a user’s identity.

One-time password technology is available in many form factors including:

- **Hardware authenticators.** Traditional hardware authenticators (sometimes referred to as “key fobs”) are portable devices that are small enough to fit on a key chain and meet the needs of users who prefer a tangible solution or who access the Internet from a number of different locations.

- **Software authenticators.** Software authenticators (for PCs, USB drives, or mobile devices) are typically offered as an application or in a toolbar format that is securely placed on a user’s desktop, laptop or mobile device.

- **On-demand.** On-demand authentication involves delivery of a unique one-time password code “on demand” via SMS (text message) to a mobile device or a user’s registered e-mail address. Upon receipt of the unique code, a user simply enters it, along with their PIN or password, to gain access.
**Risk-based authentication**

Risk-based authentication is a system that measures a series of risk indicators behind-the-scenes to assure user identities, devices, and/or authenticate online activities. Such indicators include certain device attributes, user behavioral profiles, device profiles and IP geo-location. The higher the risk level presented, the greater the likelihood is that an identity or action is fraudulent. If the system determines the authentication request to be above the acceptable risk threshold (typically established by each organization), then risk-based authentication provides the option to challenge the user with “step up” authentication. In a step-up authentication scenario, a user may be asked to answer challenge questions or submit an authorization code delivered to a phone via SMS text message or e-mail.

**Knowledge-based authentication**

Knowledge-based authentication is a method used to authenticate an individual based on knowledge of personal information, substantiated by a real-time interactive question-and-answer process. The questions presented to a user are gleaned from scanning public record databases, are random and previously unknown or unasked to the user.

**Digital certificates**

A digital certificate is a unique electronic document containing information that identifies the person or machine to which it is bound. The digital certificate can be stored on a desktop, smart card or USB. For stronger two-factor authentication, the digital certificate can be locked on a smart card or USB, requiring the user to enter a PIN in order to unlock the certificate and use the credential. The digital certificate can then be utilized to authenticate a user to a network or application. In addition to being used for user authentication, digital certificates can add value to the enterprise by enabling digital signatures or e-mail encryption.

Digital certificates can also be combined with OTP deployments using a hybrid authenticator. In this case, the hybrid authenticator stores multiple credentials and streamlines the end-user experience. A common use case for a combined certificate and OTP deployment is to unlock hard disk encryption with a digital certificate followed by authentication to a VPN with a one-time password.

**The ROI Benefits of Strong Authentication**

The perceived cost of strong authentication is misleading, and organizations that focus solely on cost overlook the long-term benefits that can be derived from implementing a strong authentication solution. Also, strong authentication is no longer just built for the large enterprise. Many vendors offer effective strong authentication solutions that fit the limited IT budgets of small and mid-sized businesses and deliver the same benefits.

Considerations that should be made in making the case for strong authentication include:

**Reduce risk**

As functionality and technology move information – and access – to new channels, the risks to information grow. As the workforce continues to mobilize, corporate “boundaries” become less distinct – as do the types of devices that are used to access the corporate network. The value of the organization’s data no longer is specific to industry or size — no business is “safe.” Strong authentication can help organizations mitigate their risk by assuring the identities of users before granting access to sensitive information and applications — regardless of the channel or device that they are using to access the information.
Enable employee mobility

Technology is making the world smaller, connecting employees with information no matter where they are in the world. As the remote and mobile channels become more refined, more employees can access the corporate network and its sensitive data – anytime, anywhere, and from a wide range of corporate-sanctioned and/or consumer devices and venues that may or may not be secure. Strong authentication offers an additional layer of protection to facilitate secure remote access to critical business systems and information – and ensure and enable employee mobility and productivity.

Creates new business opportunities

Extending applications to multiple channels, including online and mobile, has allowed organizations to provide convenient self-help services that offer real-time access and improve customer satisfaction – and offer easy, 24/7 access to information for contractors, partners and suppliers. In any online or mobile environment, it is important to establish trust with the user. Strong authentication provides organizations with the assurance that their users are who they say they are – and simultaneously builds the confidence of the user populations – in particular, the customers – who are using the services that contain their personal information.

Lower costs

Some business applications provide the ability for companies to address expensive, labor-intensive internal processes. Order processing, human resource systems, forms processing applications and numerous other personnel-intensive business processes are being automated to introduce efficiencies and reduce costs. Strong authentication enables convenient – and critical – authentication for users of these applications which are critical components of the business infrastructure. In addition, strong authentication eliminates the high volume and cost of password resets, thereby reducing the cost of help desk support.

Support Compliance

Government regulations such as Sarbanes-Oxley, PCI Data Security Standard, US Data Breach Notification laws and the Health Insurance Portability and Accountability Act are just a few of the regulations that call for the use of strong authentication to protect access to the corporate network in order to meet compliance requirements. Failure to meet these requirements could result in regulatory fines and penalties.

Conclusion

Unlike password management systems, strong authentication delivers the powerful security necessary to protect access to sensitive data – regardless of channel – and allows users to conduct business safely. The hidden costs associated with password security outweigh the perceived high price-tag of implementing strong authentication. Many security vendors provide multiple strong authentication solutions for companies of all sizes, including cost-effective solutions built specifically for businesses with limited IT budgets. Moving away from cost-based thinking to the benefits that can be realized with enhanced security creates a compelling case to show the return on investment from strong authentication.
### Debunking the Myths of Strong Authentication

<table>
<thead>
<tr>
<th>Myth</th>
<th>Reality</th>
</tr>
</thead>
<tbody>
<tr>
<td>I use passwords because they don’t cost me anything.</td>
<td>Passwords are actually expensive to manage when you consider that nearly 30 percent of calls placed to the help desk are for password resets. When the average cost of a help desk call is factored in, passwords actually come with many hidden costs.</td>
</tr>
<tr>
<td>My business uses strong passwords and our employees are required to change them on a regular basis, so this lowers my risk.</td>
<td>Strong passwords that include numbers, capital letters or characters are harder for a hacker to guess, but also harder for employees to remember. This creates a spike in help desk calls and leads employees to engage in unsafe password management practices, such as writing down passwords on paper, which actually increases risk.</td>
</tr>
<tr>
<td>My business can’t afford the cost of strong authentication.</td>
<td>Strong authentication can be very cost-effective – and not just for large organizations. Many vendors offer packages that carry the benefits of enterprise-level strong authentication security, but that are developed specifically for the needs – and limited IT budgets – of small and mid-sized businesses.</td>
</tr>
<tr>
<td>The cost of strong authentication outweighs the benefits.</td>
<td>The cost of strong authentication is much lower than what it would cost if your organization experiences a data breach or the fines and penalties you will have to pay for being non-compliant. In addition, strong authentication supports the move to new channels for which can open the door for new business opportunities and revenue streams.</td>
</tr>
<tr>
<td>Cyber threats only target large organizations and the government.</td>
<td>In fact, it’s quite the opposite. Cybercriminals are targeting small and mid-sized businesses on a frequent basis because they usually have limited security controls in place – such as weak password authentication – making them more vulnerable to an attack.</td>
</tr>
</tbody>
</table>
About RSA

RSA is the premier provider of security, risk and compliance solutions, helping the world’s leading organizations succeed by solving their most complex and sensitive security challenges. These challenges include managing organizational risk, safeguarding mobile access and collaboration, proving compliance, and securing virtual and cloud environments.

Combining business-critical controls in identity assurance, data loss prevention, encryption and tokenization, fraud protection and SIEM with industry leading eGRC capabilities and consulting services, RSA brings trust and visibility to millions of user identities, the transactions that they perform and the data that is generated.