Remove Your Biggest Security Risk
with the Sphinx Software

What represents the biggest risk for IT security?

Logging on to computers, websites, and applications by typing in user names and passwords causes a vulnerability…

- which is exposed because of the limits of our human capabilities -

…that is *by far* the weakest link in IT security.

We call this vulnerability the "Password Problem".

Fact: Strong passwords provide strong security.
Random, complex, and unique.

Fact: It's impossible to remember strong passwords.
Limited as we are by our human capabilities.

Fact: Hence, lax password security is the
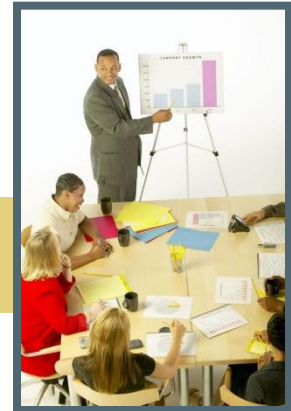*single most commonly exploited security breach.*

I

This presentation covers:

I
The Password Problem

II
How Sphinx Solves the Password Problem

III
Why Choose Sphinx?

How is your organization vulnerable?

- **Most users choose weak passwords**

  Commonly selected passwords are weak and easy to break - colors, birthdays, names of family members and pets ...

- **Most users have bad password habits**

  * *Using the same password for all logons - both corporate and personal - exposing multiple accounts at once*

  * *Writing passwords on sticky notes or calendars*

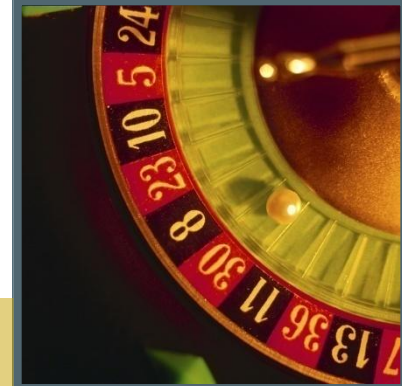- **Bottom line: passwords no longer protect**

Don't take a chance:
The time to enable employees
to use strong passwords

- An estimated 99% of all logons call for user names and passwords

This is not expected to change in the near future.

- Hackers can crack most passwords in under a minute

Well-chosen passwords could take years - if not decades - of computer time to crack.

The risk is posed by:

Insiders

Who are in close proximity and are familiar with the organization, the people, and the systems.

Outsiders

Who can have very sophisticated ways of cracking passwords.

An Insider Working with an Outsider

A potentially dangerous combination.

Insider threats are a concern that every organization must take seriously:

40% of IT security breaches are perpetrated by people inside the company.
(ZDNet)

44% of respondents in a survey of IT executives identified internal breaches as a key security challenge over the past 12 months.
(Network World)

The Password Problem

Outsider threats from hackers pose
too great a danger to be ignored:

For hackers who are able to gain
access to a corporate computer, bad passwords
are a treasure trove.

Passwords discovered on one server will frequently
open the way to other servers.

With the digital keys to a large fraction of the accounts on the
network, an intruder can wander about with impunity and with
the appearance of being a legitimate user.

(CNET)

Once unauthorized individuals gain access,
they can potentially:

Send spam

Start viruses

Steal identities

Read business and personal communications

Set up botnets and platforms for further hacking

Download large amounts of proprietary and sensitive information

The good news:
The Password Problem can be solved.

Homeland Security recommends that IT managers should:

Provide users with a password manager program.

* *Enables users to use complex, unique passwords for each logon location, since they no longer need to remember them.*

* *Makes it easy to change passwords frequently.*

Incorporate two-factor authentication.

Requires an additional level of authentication, such as a hardware security token (something you have) and a PIN (something you know).
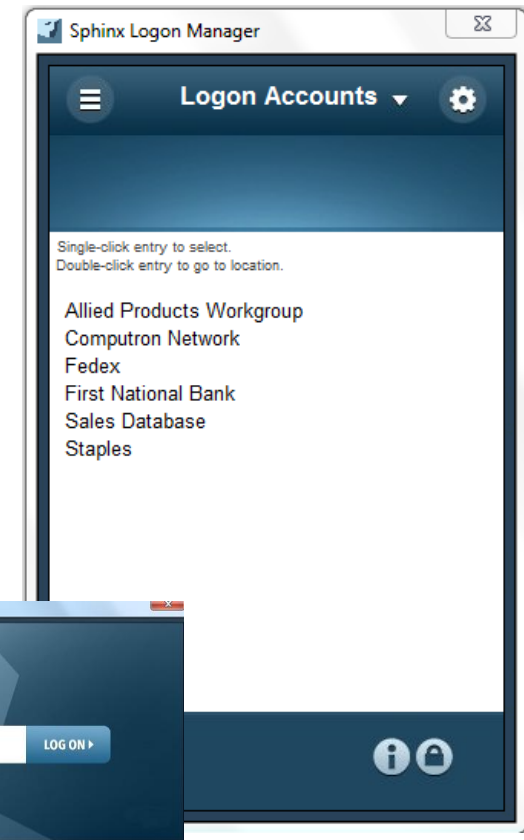
II

The Sphinx software provides the two key security elements recommended by Homeland Security:

Password management

Two-factor authentication

Plus, Sphinx provides an additional key security element that sets it apart from the field:

"Smart card secure" protocols

The next three slides look at these elements in more depth…

KEY SECURITY ELEMENT 1

Password management

- Stores user names and passwords securely for logon to Windows, websites, and applications.

- Transfers logon data to target location transparently - data entry cannot be observed and thus reproduced.

- Makes it easy to store logon data and create strong passwords with features such as "auto-record", "auto-fill", and "create password".

KEY SECURITY ELEMENT 2

Two-factor authentication

- Uses smart card or RFID card to store logon data.

- Employee must present card and enter PIN to gain access to stored data.

- This level of "strong authentication" is now required by many federal regulations and industry standards organizations.

KEY SECURITY ELEMENT 3

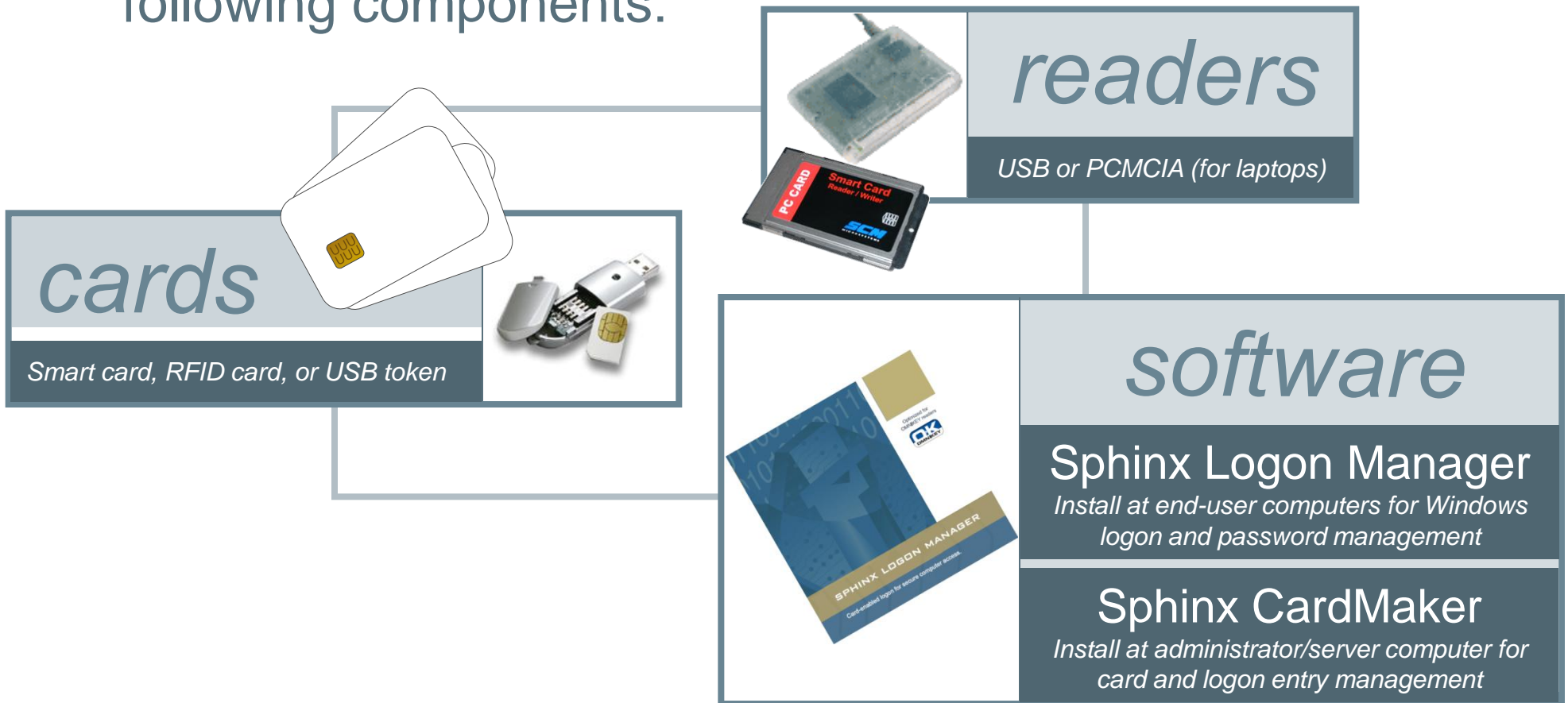## "Smart card secure" protocols

- Built on the stringent secure protocols of the smart card industry. A simple password program can't compete with this level of security.

- Whether data is stored on a smart card or secreted away on the secure server, it's iron clad by layers of encryption at every turn.

- Tough multi-key challenge/response protocols ensure only authorized transactions succeed.

A complete Sphinx installation requires only the following components:

readers

USB or PCMCIA (for laptops)

cards

Smart card, RFID card, or USB token

software

Sphinx Logon Manager

Install at end-user computers for Windows logon and password management

Sphinx CardMaker

Install at administrator/server computer for card and logon entry management

The next section provides six reasons why so many customers choose Sphinx:

1. Easy to install

2. Easy to use

3. High quality

4. Full featured

5. Saves money

6. Interoperability

Why Choose Sphinx?

Easy to install	Easy to use	High quality	Full featured	Saves money	Interoperability

Reason 1: Sphinx works out-of-the-box

Fits into your current setup

An "add on" solution rather than an "infrastructure" solution.

➤ *Fits into the secure Windows environment and protocols that you've already established, with no need for infrastructure changes.*

Saves you setup time and effort

Compare with competing "infrastructure" solution products that must be integrated into your environment.

➤ *Some competitors boast when setup is completed within 3 months, and charge you every step of the way.*

Ready for use in minutes

All components work together out-of-the-box.

➤ *Run with preset default settings. Or, easily modify security settings and policies to tailor-fit your organization.*

III

| Easy to install | Easy to use | High quality | Full featured | Saves money | Interoperability |

Reason 2: Sphinx is built for ease of use

Easy to manage cards

End-users self enroll, or administrator issues cards with two mouse clicks.

➤ *For lost and stolen cards: simply add to "hotlist" and re-issue, or let cardholder self re-enroll.*

Synchs with Active Directory

Windows password changes are synchronized, whether you update as prompted by Windows, or in Sphinx.

➤ *Works with Active Directory in a non-intrusive way, ensuring logon integrity for all users.*
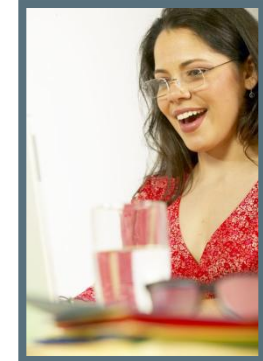
Popular with end-users

High acceptance rate, because Sphinx makes it so easy for end-users to employ strong passwords.

➤ *Simple screens and functions are self-explanatory.*

Easy to install	Easy to use	High quality	Full featured	Saves money	Interoperability

Reason 3: Sphinx is serious about security

Every step is secured

From the card to the secure server, you can be confident that your data is secured with the best available methods.

➤ *Challenge/response, random number generation, and data encryption keep your data safe.*

Proven around the world

For almost ten years, the Sphinx software has been continuously refined and improved to optimize the data security of our customers - from Fortune 500 companies to doctor's offices.

➤ *Sphinx has the seasoned experience to deliver "the logon security you need, with the simplicity you want".*

Security is what we do

Since 1996, Open Domain has provided specialty software for critical data security processes, specializing in smart card technology.

➤ *We are known in the industry for the quality of our work.*

Why Choose Sphinx?

Reason 4: Sphinx is packed with features

End-user features

With the Sphinx Logon Manager software, end-users can save logon entries for Windows, websites, and applications, plus:

- *Make strong random passwords by clicking on "Create" button.*
- *Pull card to lock, logoff, or shutdown computer.*
- *Securely store address and payment information for "dragging and dropping" into web fields.*
- *And much more…*

Administrator features

With the Sphinx CardMaker software, administrators can manage cards and cardholders, plus:

- *Control PIN and password policies, and define user groups.*
- *Create and manage logon entries for end-users.*
- *View log of cardholder logon and logoff.*
- *Print cards as part of card issuance.*
- *And much more…*

Plus…

- *PKI option.*
- *Biometric authentication.*
- *And much more…*

Please see our complete Feature List to view all that Sphinx has to offer at: *www.odsphinx.com*

| Easy to install | Easy to use | High quality | Full featured | Saves money | Interoperability |

Reason 5: Sphinx saves money in more ways than one

Low "one fee" pricing

Sphinx' single license fee - based on number of cardholders - includes both the end-user and the administrator software, plus the complete feature pallette.

➢ *Sphinx is often a fraction of the cost of competing solutions that charge separate fees for end-user and admin software, feature modules, etc.*

No setup or ongoing fees

Since Sphinx is an "add-on" solution, you can quickly complete setup and maintain the solution yourself.

➢ *No need to pay installers to integrate the software with your environment, and no ongoing integration fees.*

Time is money

For employees: No more valuable time wasted trying to remember or find passwords.

For administrators: Greatly reduces logon support calls from forgotten passwords.

Why Choose Sphinx?

III

Reason 6: Sphinx is committed to interoperability

Non-proprietary

Sphinx is the choice of customers who don't want to commit to the potential limitations and price control of one proprietary vendor.

➤ *Works with a wide variety of industry standard cards and readers.*

Open standards

Built around open API standards to provide interoperability between platforms, hardware, and third-party software solutions.

➤ *Sphinx' open "hooks" make it easy to build in to third party solutions, if desired.*

Dedicated to teamwork

We are always eager to consider new compatibility options that benefit the market.

➤ *Optimizing solutions for customers and partners is a priority.*

III

In conclusion, a summary of Sphinx' benefits:

☑ **Makes it easy to solve the "password problem",**
keeping company data safe and protecting employees' identities.

☑ **Simple to "add on" to your existing Windows environment,**
and works out-of-the-box with compatible cards and readers.

☑ **Greater employee productivity, less logon support calls.**

☑ **High quality, high performance, full-featured product**
for a reasonable price from a non-proprietary vendor.

☑ **Strong two-factor authentication**
meets the security requirements of many regulatory agencies, such as HIPAA.

Appendix A: System requirements

Operating system:

End-user computers:	Windows Vista, 7, 8, 8.1, 10.
Admin/server computer:	Windows Server 2003, 2008, 2012.

Browser:

End-user computers:	Internet Explorer, Chrome, Firefox.

Appendix B: Card choices

Smart card	• Standard ID card format, can be printed • Use in "on card mode" or "server mode"
Smart token	• Attractive compact format • Use in "on card mode" or "server mode"
RFID card	• Use existing building access cards for logon • Use in "server mode" to keep data safe

Card choice 1:

Smart card

The choice of high security organizations, now easily affordable for all.

Options	• Inexpensive smart chip card, or PKI capable card • Inexpensive desktop reader, or PCMCIA reader (for laptops)
Usage	• *If data portability is more important:* Use in "on card mode", where data is stored on the card • *If management control is more important:* Use in "server mode", where data is stored on the secure server, so administrator can control managed entries, etc. • Or, use a combination of both modes
Tip	• Delivers the most "bang for the buck" if you want an ID card format • Available as white cards, or pre-printed with an ID# and your logo

Card choice 2:

Smart token
Protects your data in a way that a simple data storing token cannot.

Options	• USB smart token with inexpensive smart chip • USB smart token with PKI capable chip
Usage	• *If data portability is more important:* Use in "on card mode", where data is stored on the card • *If management control is more important:* Use in "server mode", where data is stored on the secure server, so administrator can control managed entries, etc. • Or, use a combination of both modes
Tip	• Inexpensive option • Attractive, compact format is popular with end-users

Card choice 3:

RFID card
Use the same card to secure building access and computer access.

Options	• Mifare, HID, or Indala building acess cards • If you already use one of the above cards, Sphinx can be used with no change to your card infrastructure
Usage	• Use in "server mode", where data is stored on the secure server, so administrator can control managed entries, etc. • Or, adding a smart chip to your RFID card adds data portaility and/or enables you to use inexpensive readers
Tip	• Available as white cards, or pre-printed with an ID# and your logo • Be aware that the cost of RFID card readers is higher than smart card readers. This is not such a consideration however, if multiple cardholders are using a single PC.