InformationWeek
WEBCAST

Hardening Private Keys with Less Hassle, Less Cost and More Security: A Case Study in Authentication

An InformationWeek Webcast

Sponsored by

TRUSTED
COMPUTING GROUP™

UBM
TechWeb

Featured Speakers

Kirk Laughlin, Contributing Editor, InformationWeek

Karl Wagner, Director of Global Networking & Telecommunications, PwC

Mark Lobel, Partner (Principal), PwC

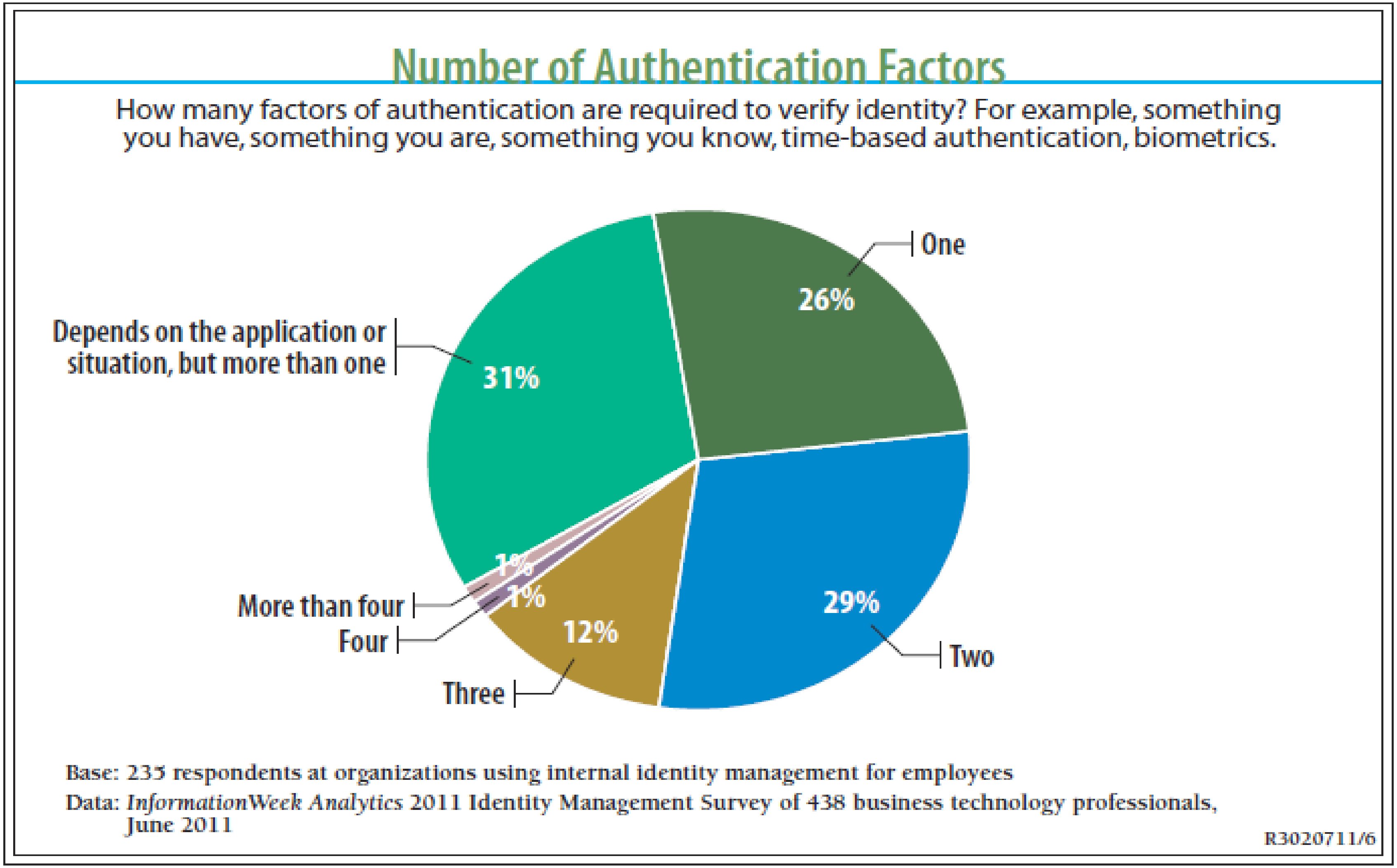
Apurva Bhansali, CEO & CTO, Softex

Getting the Most out of Authentication and ID Management

Kirk Laughlin,

Information Week, Contributing Editor

UBM
TechWeb



Number of Authentication Factors

How many factors of authentication are required to verify identity? For example, something you have, something you are, something you know, time-based authentication, biometrics.

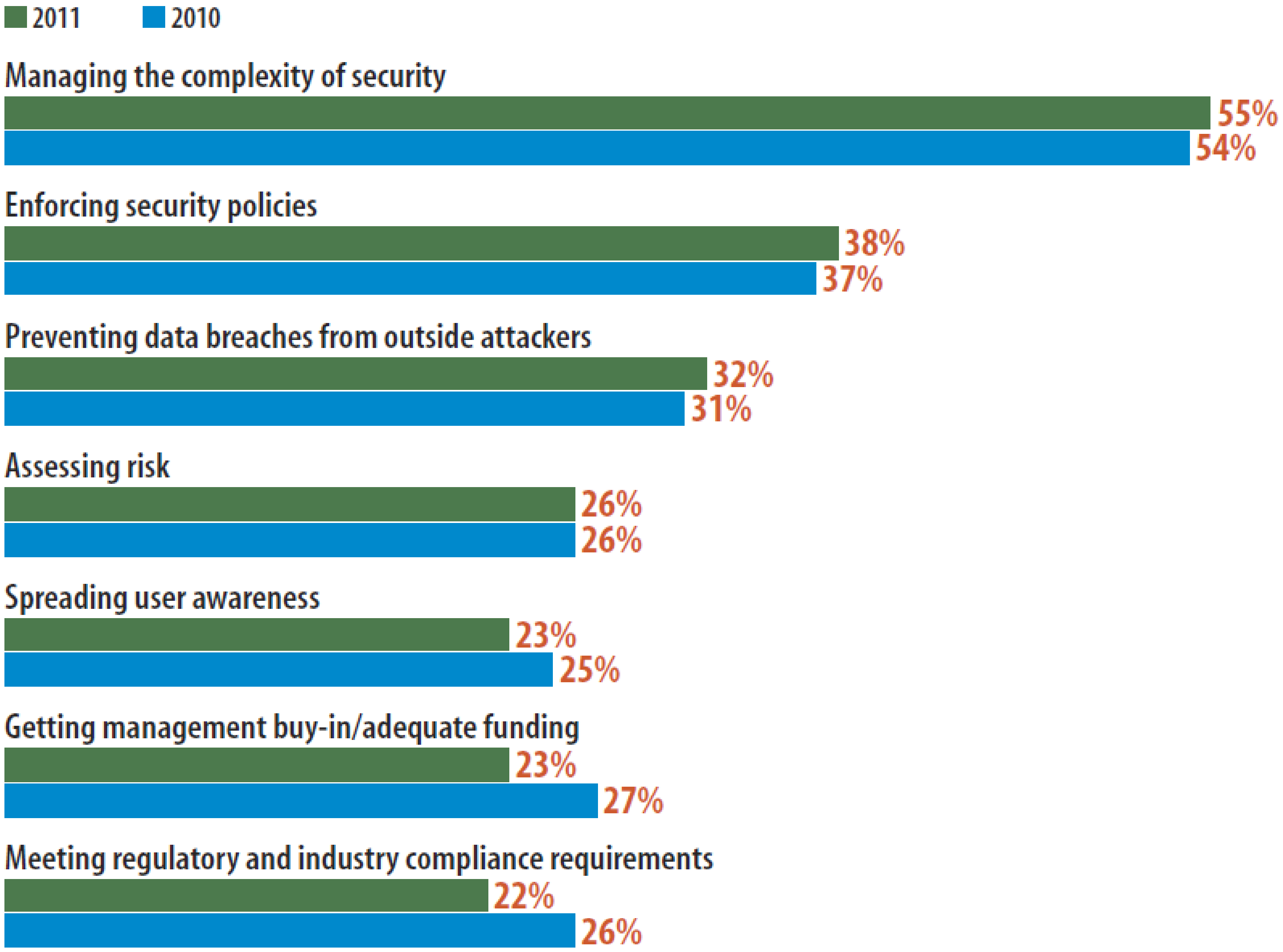
Base: 235 respondents at organizations using internal identity management for employees

Data: *InformationWeek Analytics* 2011 Identity Management Survey of 438 business technology professionals, June 2011

R3020711/6

Biggest IT Security Challenges

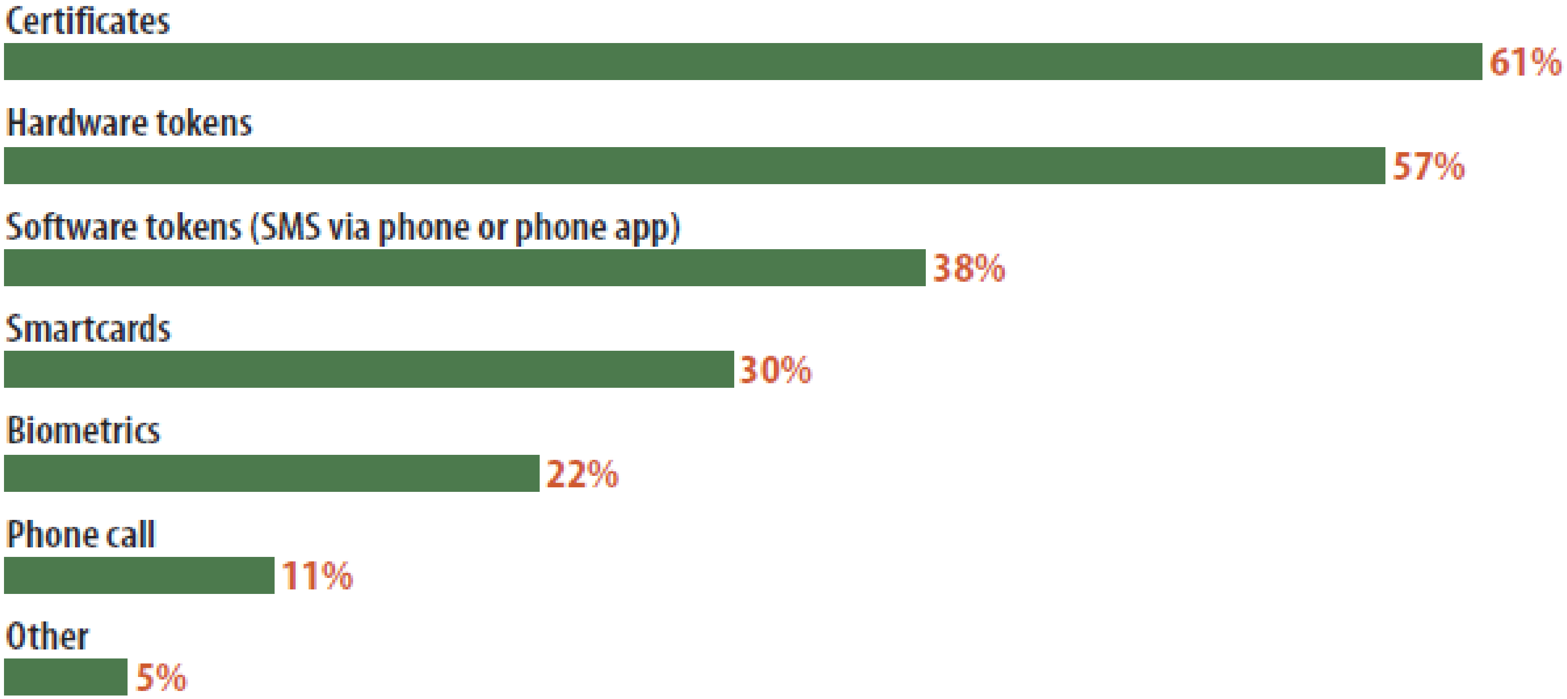
Which of the following are the biggest information/network security challenges facing your company?



TechWeb

Authentication Factors in Use

What technologies do you use for additional authentication factors?



Note: Multiple responses allowed

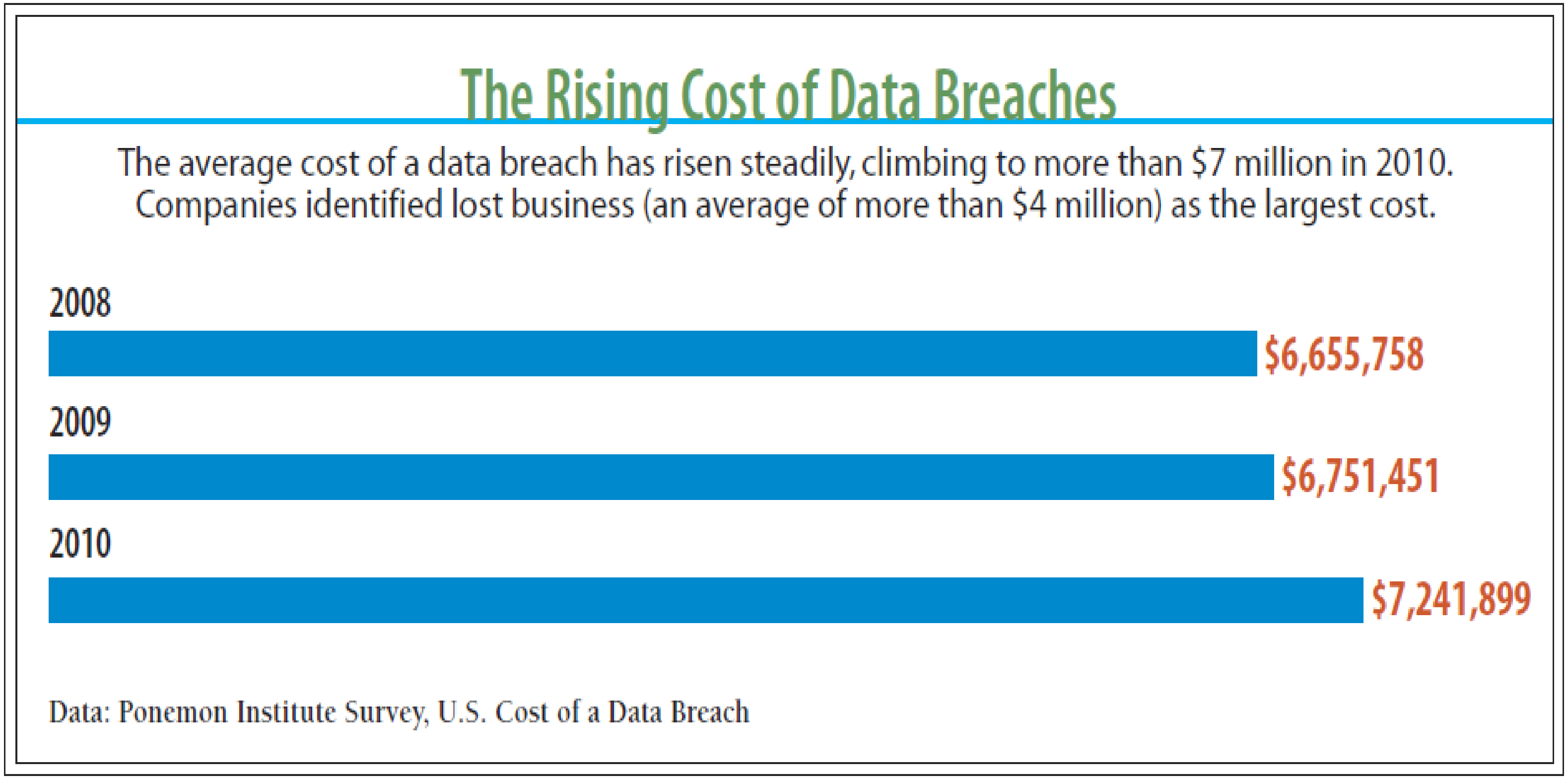
Base: 175 respondents at organizations using internal identity management for employees and requiring more than one factor of authentication

Data: *InformationWeek Analytics* 2011 Identity Management Survey of 438 business technology professionals, June 2011

R3020711/7

Breaches are Getting Costly

Figure 3



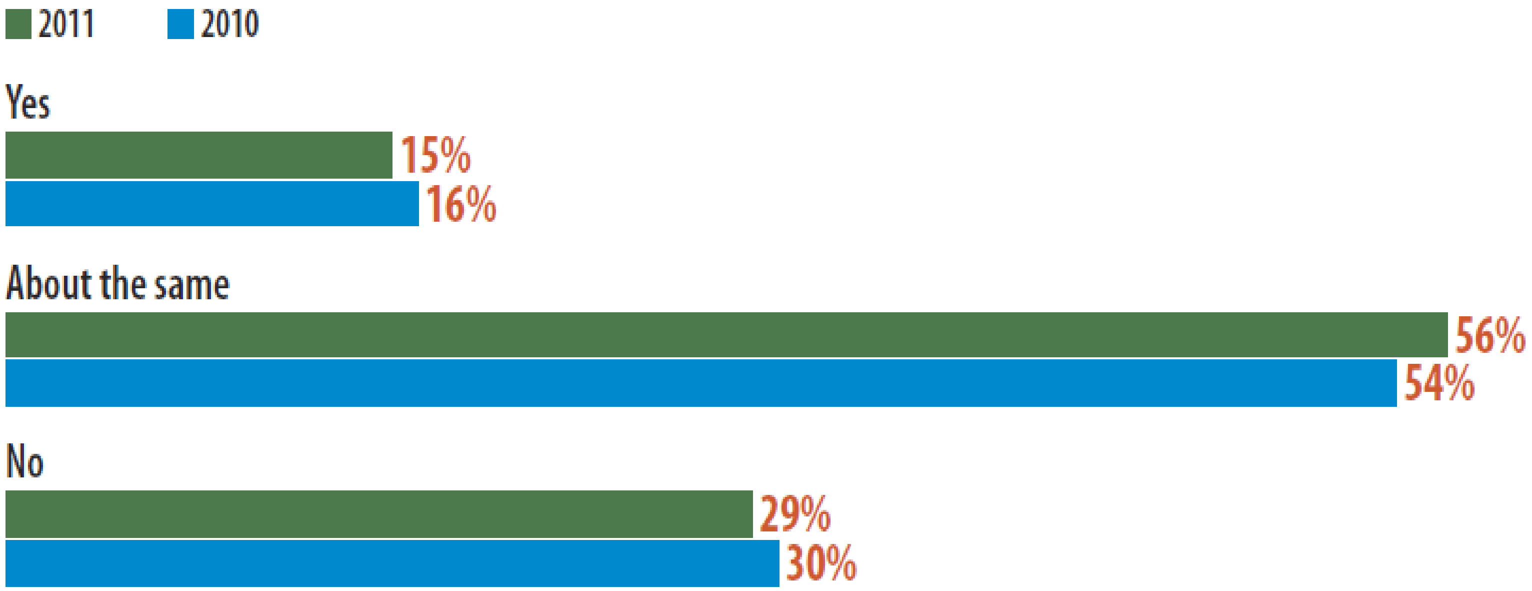
The Rising Cost of Data Breaches

The average cost of a data breach has risen steadily, climbing to more than $7 million in 2010. Companies identified lost business (an average of more than $4 million) as the largest cost.

Data: Ponemon Institute Survey, U.S. Cost of a Data Breach

More Vulnerable to Security Breaches?

Is your organization more vulnerable to malicious code attacks and security breaches than it was a year ago?



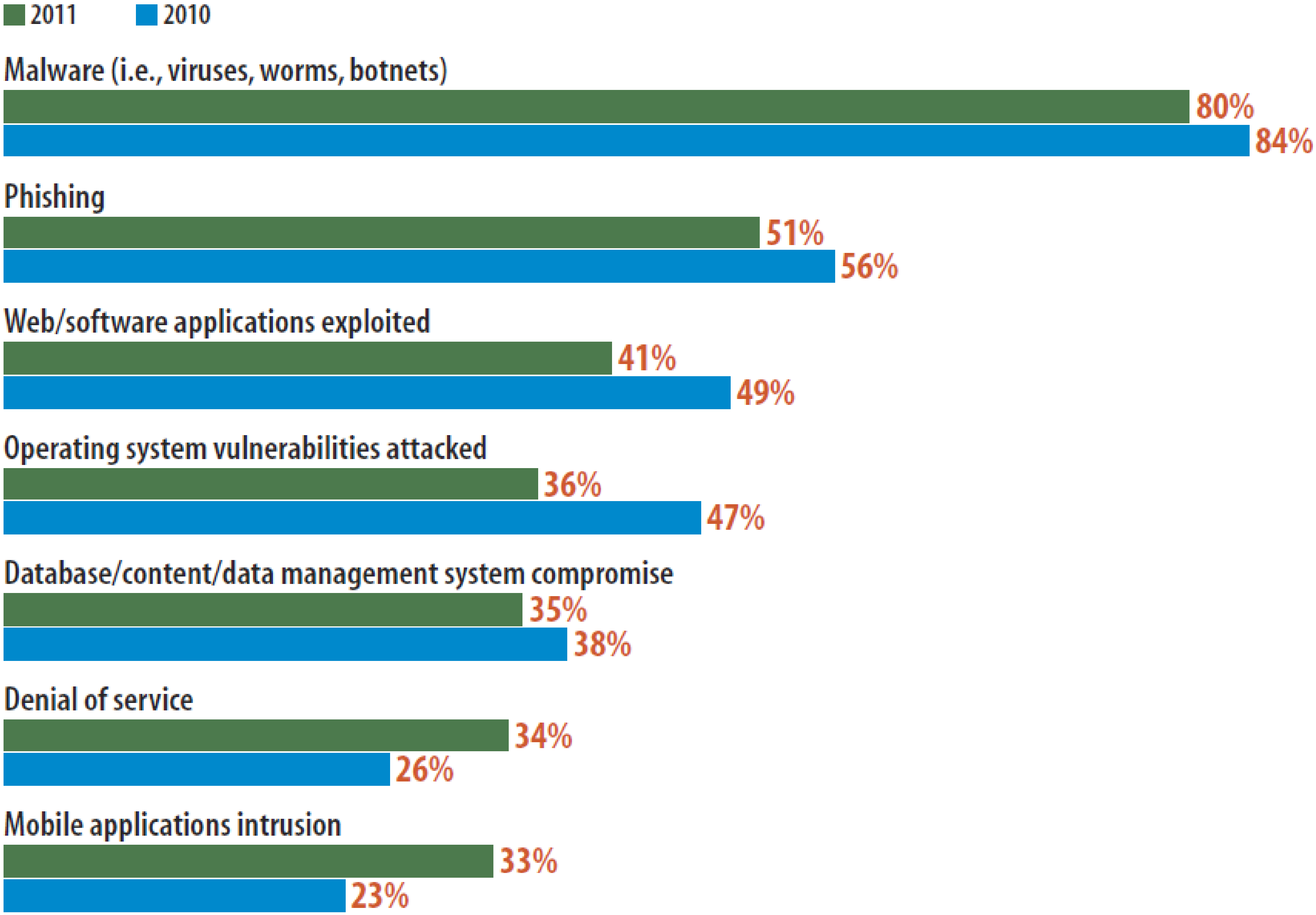
Base: 1,084 respondents in March 2011 and 1,002 in April 2010

Data: *InformationWeek Analytics* Strategic Security Survey of business technology and security professionals

R2120511/2

Types of Breaches Most Likely to Occur

Looking ahead, which types of security breaches or espionage are most likely to occur in your organization within the next year?



Tips: Stronger Authentication / ID Management

- Work business partners to put baseline IdM police guidelines in place *before* granting remote access
- Allows administrators to create policies regarding user IDs, such as password strength
- Establish priorities in pursuit of IdM plan
- Ensure IdM integrates into physical security
- Create consistent benchmarks

Low Cost, Strong Authentication at PwC
Our Journey

Karl Wagner, Director of Global Networking & Telecommunications, *PwC*

Mark Lobel, Partner (Principal), *PwC*

Where We Started

The Challenge (e.g. Problem):

- Multiple authentication systems that were individually chosen
  - Mix of PKI/Private Key & One Time Password (OTP) systems
  - End users faced multiple interfaces for authentication
  - Total cost of all authentication systems high

Where We Started

The Challenge (e.g. Problem):

- Our existing authentication technology used started to become vulnerable
  - One of our internal security groups had successfully broken through one of our soft token (OTP) systems
  - Jailbreak software had been developed for the Windows O/S private key storage
- Degraded the strength of our two factor authentication systems

What We Wanted

Objective:

- Reuse common systems to keep costs low – both initial and ongoing costs
- Flexibility to accommodate the widest range of needs practical
- Provide tamper resistant hardware protection to eliminate many software based vulnerabilities

What We Wanted

Two Factor Authentication:

"Something you know" + "Something you have"

- "Something you know" is your userID and password
- "Something you have" could be:
  - Private key associated with a certificate
  - OTP seed data
  - A device that stores OTP seed data or Private keys or both
- We avoided "Something you are" (biometrics) because it can't be changed or revoked

Key Decisions

Separate internal and external solutions?

- Internal users have devices managed by PwC
- Software and configurations can be changed on devices for internal users
- External users have devices not managed by PwC– no updating allowed
- Internal security policies treated internal and external differently

Answer: Separate internal and external

Key Decisions

Use PKI or OTP Tokens?

- PKI is natively supported in more situations than OTP
  - Wireless LANs in offices – EAP-TLS, EAP-PEAP, etc.
  - Web applications & Remote Access VPN – SSLv3
  - Support of OTP exists as an afterthought
- PKI can be used for single factor as well as two factor authentication

Key Decisions

Use PKI or OTP Tokens?

- OTP Token solutions frequently require additional software on servers and/or clients – makes upgrades complicated
- PwC's PKI systems were operating at about half the cost of our OTP systems
- Difficult to deploy PKI for external users

Answer: PKI for internal user SMS tokens or Knowledge Based Authentication (KBA) for external user

Key Decisions

What do we use for PKI tamper resistance?

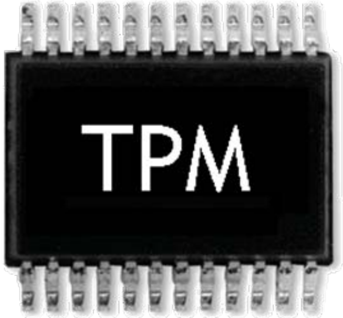
- 3 Options: Trusted Platform Module (TPM), SmartCard or USB Dongle
- No application changes needed for TPM, SmartCards nor USB dongles
  - Use Microsoft CAPI for compatibility
- TPM lowest cost: TPM=1x SC=2x USB=3x
- Can’t lose my TPM - it’s part of the laptop
- TPM is restricted in a few countries

Key Decisions

What do we use for PKI tamper resistance?

- Additional step to clear TPM for old PCs
- TPM has no additional shipping/logistics
- TPM can’t be moved to a different device

Answer: TPM for Windows PCs, SmartCard or USB in restricted countries (CN, RU) or for Mac O/S.

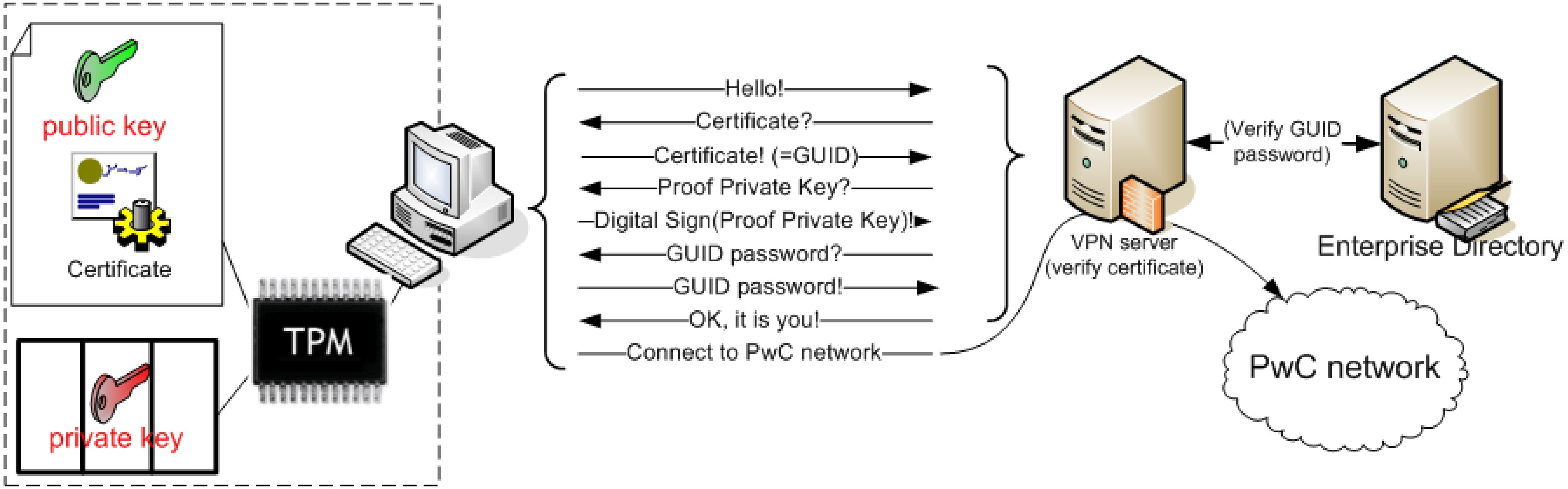


About TPM

- Already in our laptops
  - 350 million TPMs deployed worldwide
- Is based on open standards
- Gives FIPS 140-2 level 3 protection
- Free - no hardware costs
- Protects against ”Jailbreak” and similar tools
- Minor changes in PC Lifecycle Management. TPM setup in a few minutes
- PwC applications worked well with TPM, often with no coding changes

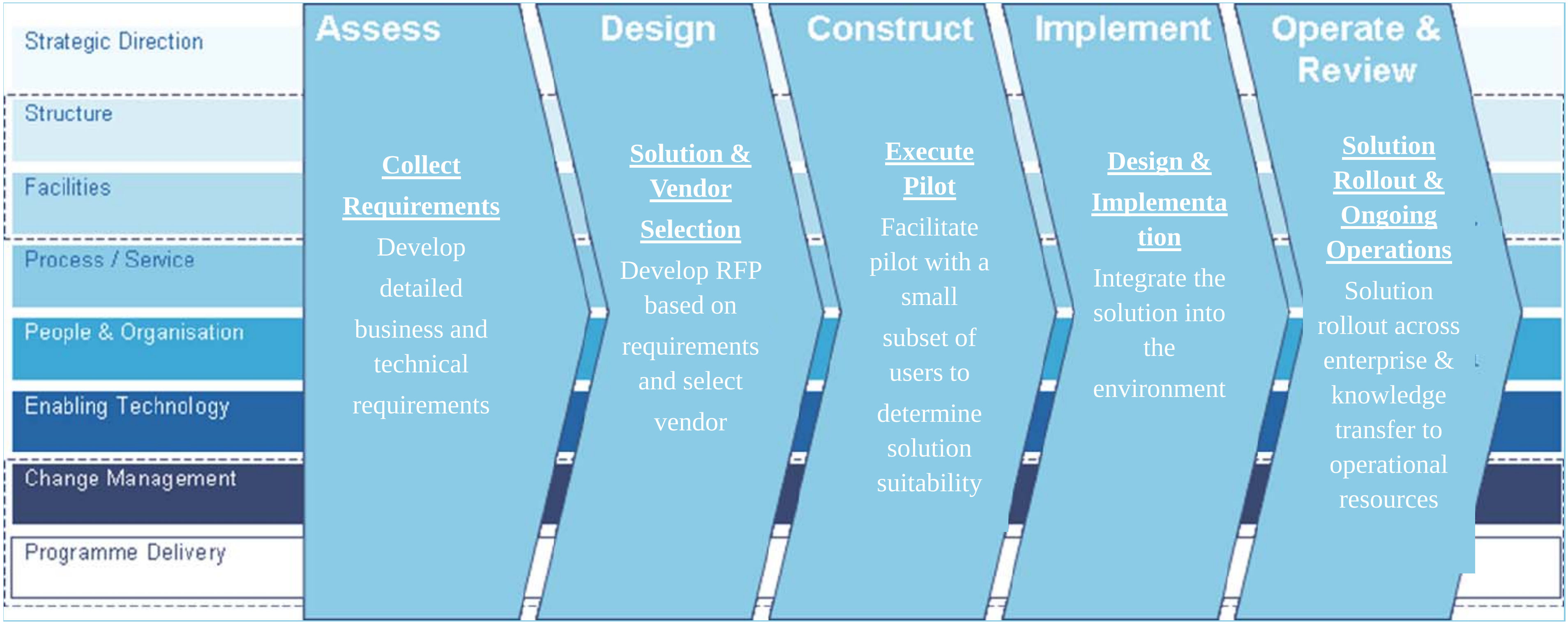
Example Results - RA VPN

- When you want to connect to the PwC network through VPN, you need:
    1. Digital Certificate and Private Key (1st factor, "have")
    2. Know your "PIN" to unlock you private key (only for VPN, not for WiFi)
    3. GUID and GUID password (2nd factor, "know")
- No changes to the VPN infrastructure when using TPM and no Jailbreak vulnerability anymore!



Lessons Learned

Take a multi-phased approach to implement multi-factor authentication solutions



Collect Requirements
Develop detailed business and technical requirements

Solution & Vendor Selection
Develop RFP based on requirements and select vendor

Execute Pilot
Facilitate pilot with a small subset of users to determine solution suitability

Design & Implementation
Integrate the solution into the environment

Solution Rollout & Ongoing Operations
Solution rollout across enterprise & knowledge transfer to operational resources

Lessons Learned

Key steps in deployment

- Determine requirements for two-factor authentication from key stakeholders
- Conduct a current state ("as-is") analysis of two-factor authentication and supporting processes
- Design future state of multi-factor authentication along with supporting processes. Solution design will take into account multiple user communities including service accounts, administrators, contractors etc.
- Select a flexible and scalable vendor solution that supports requirements
- Integrate solution management with existing Identity management system
- Ensure that the selected solution is compliant with relevant legal and regulatory requirements
- Develop end user deployment strategy, including change management and communication.
- Provide detailed and comprehensive framework to support operational process components (i.e. issuing cards, lost cards, training, policy and procedures, etc)
- Develop documentation to support rapid solution integration at other businesses

Lessons Learned - Key Questions

Business

- Is the solution currently supported in organizations operating in multiple countries/regions?
- Are other large conglomerates/industry peers using this vendor?
- Is the solution scalable?
- What are the impacts to user experience if this solution is deployed?
- Is the registration process implicit, transparent, history based or explicit/formal?

Technology

- What are the additional hardware/software (smart card readers/GINA modifications/CSP additions) requirements for a functioning solution in your environment (Windows/Unix)?
- What is lost/stolen cards/token process?
- How is the authenticating information stored on the token/smart card (plain text/encrypted)? How are the end-user private keys protected (pin/password/biometric)?
- Has the solution been integrated for provisioning with an Identity management solution? What is the extent of integration (automated, notification based)
- What application integration methods (e.g. API, redirect/filter, agent, etc.) are supported?

Lessons Learned

	Areas of Concern	Critical Success Factors
Project/ Program Structure and Approach	· Project led by technology group without high-level partnership with the business · No business executive sponsorship · Failure to understand enterprise nature of multi-factor authentication solutions · 'Boil the ocean' scope and approach – 'big losses' vs. 'quick wins' · Failure to set realistic expectations	· Active high-level business executive sponsorship · Clear project/program charter defined · Clear definition of roles and responsibilities · Agreed upon guiding principles and objectives · Short-term, mid-term and long-term milestones · Dependencies and inter-dependencies well understood · Broadly accepted success criteria
Organization and People	· The processes, technology and people span across multiple geographies, business units and functional areas – priorities, objectives and agendas are not always aligned · Lack of resources and experience to adequately build and maintain solution · Operational impact is not fully contemplated during planning and design phases – technical and end user	· Business and IT ownership/sponsorship · Communications and change management integration within program · Define roles and responsibilities – entire lifecycle · Training – technical, functional and end users
Process and Data	· Lack of documented understanding of current and future state processes · Regulatory and compliance risks – over or under controlled · Data management challenges – what to protect? How much to protect?	· Document and maintain current process workflows · Develop new process use cases before project requirements · Address data issues first
Technology	· Product selection is 'the strategy' · Rushing to implement product before business requirements are defined · Buying into vendor rhetoric – it's not simple · Poor understanding of the scale and impact of the technology	· Select solutions after business requirement and processes are defined and accepted · Form strong, open relationships with implementer and vendor(s) · Test, pilot and test again!

Multi-Factor Authentication Strategy

Apurva Bhansali, CEO and CTO, *Softex*

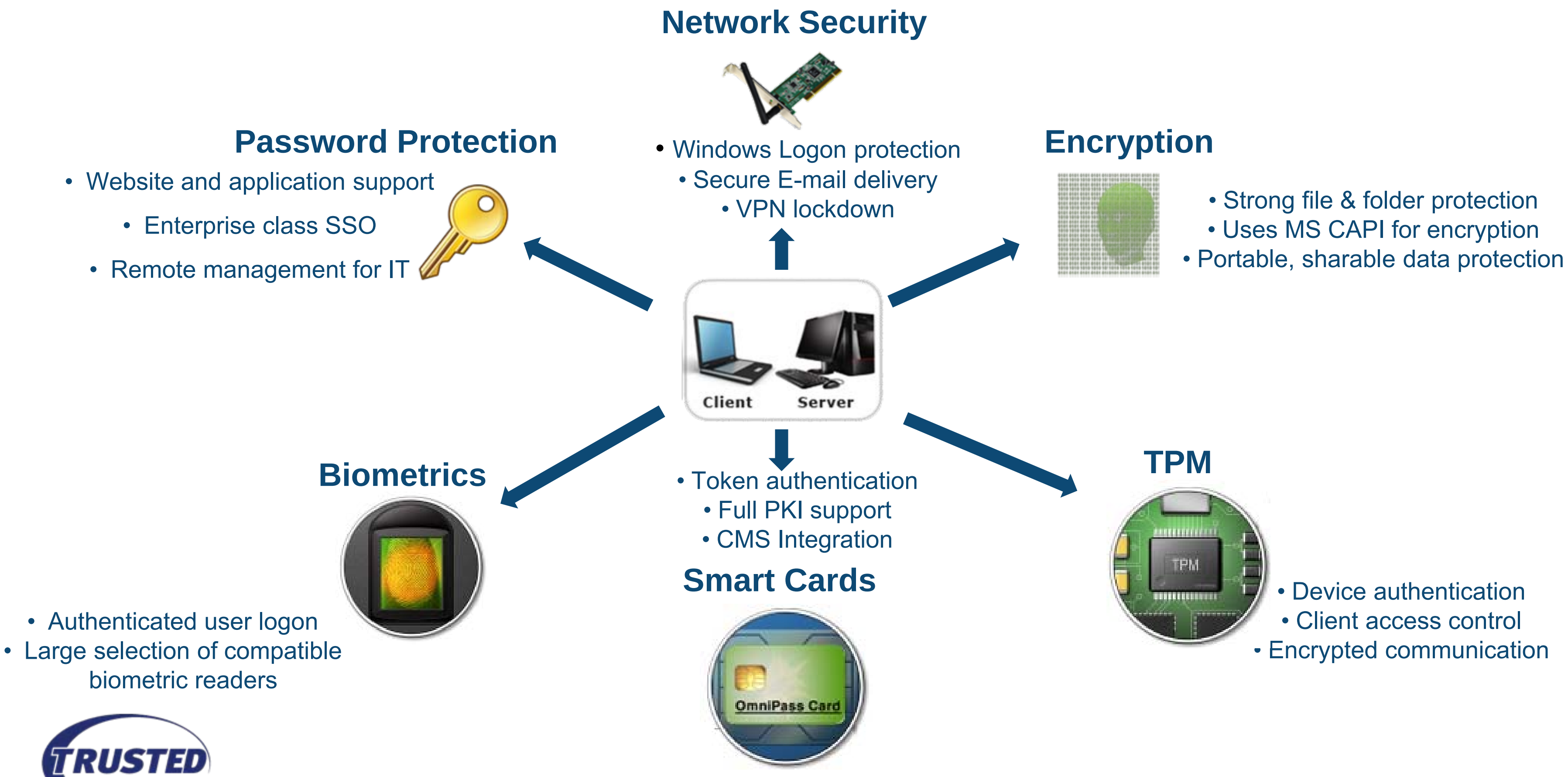
Authentication Problem

The Pain Points:

- Passwords can be easily compromised
  - A compromised password can potentially compromise data, applications and networks accessed by the PC, even if encryption is used
  - Cost of compromise cannot be calculated
    - Best case – strong fines for potential violations
    - Worst case – public disclosure embarrassment, high resolution cost
- Passwords have a high TCO
  - Resetting passwords alone can cost an organization $21 per call to help desk (per Gartner Research); employee downtime, cost of maintaining IT infrastructure, etc

Multi-factor Authentication

Security and convenience to individuals and enterprises can be provided using strong authentication technologies and multi-factor authentication.



Network Security

- Windows Logon protection
- Secure E-mail delivery
- VPN lockdown

Password Protection

- Website and application support
- Enterprise class SSO
- Remote management for IT

Encryption

- Strong file & folder protection
- Uses MS CAPI for encryption
- Portable, sharable data protection

Biometrics

- Authenticated user logon
- Large selection of compatible biometric readers

Smart Cards

- Token authentication
- Full PKI support
- CMS Integration

TPM

- Device authentication
- Client access control
- Encrypted communication

Authentication Case Study

Customer:

- One of the oldest and largest partnership bank in America. It currently operates in eight domestic and seven overseas location with over 3000 employees.

Problem:

- Securing data and transactional information, both from a fiduciary and regulatory perspective
- Employees had multiple passwords to corporate applications – 100+ applications (Green Screen, SAP, Legacy, etc)
- Huge costs related to password reset calls to IT Helpdesk – 3-5 resets per employee per year
- Password compromise caused data security issues

Challenge:

- Eliminate dependence on multiple passwords
- Reduce IT support demands
- Comply with regulatory requirements

Authentication Case Study (Contd)

Solution:

- Enterprise-wide deployment of Softex OmniPass Enterprise Single Sign On Solution
- Eliminate passwords with strong multi-factor authentication – TPM and Biometrics

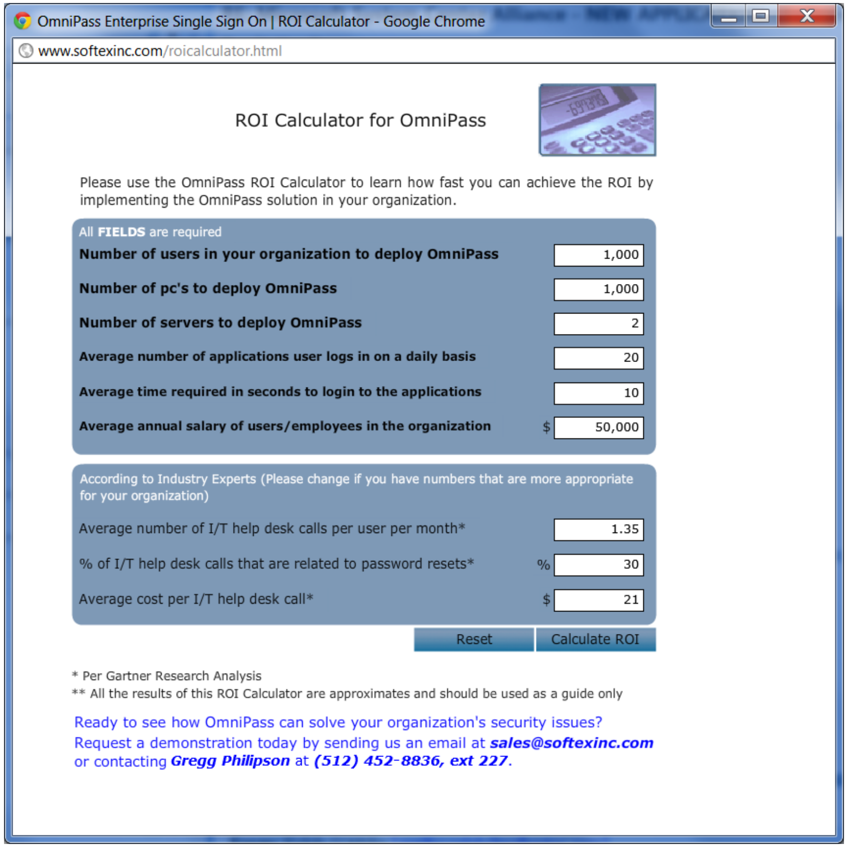
Results:

- Lowered password reset costs – reduced reset calls by 98%
- Increased staff productivity
- Reduced security risks
- Facilitated regulatory

Customer Quote:

“OmniPass was easy and quick to install. If we go with a biometric solution in the future, this would be an easy transition. Softex has given us a tool that allows users to manage their passwords and allows us to decrease the risk of social engineering security issues”

Authentication ROI Calculator


OmniPass Enterprise Single Sign On | ROI Calculator - Google Chrome
www.softexinc.com/roicalculator.html

ROI Calculator for OmniPass

Please use the OmniPass ROI Calculator to learn how fast you can achieve the ROI by implementing the OmniPass solution in your organization.

All **FIELDS** are required

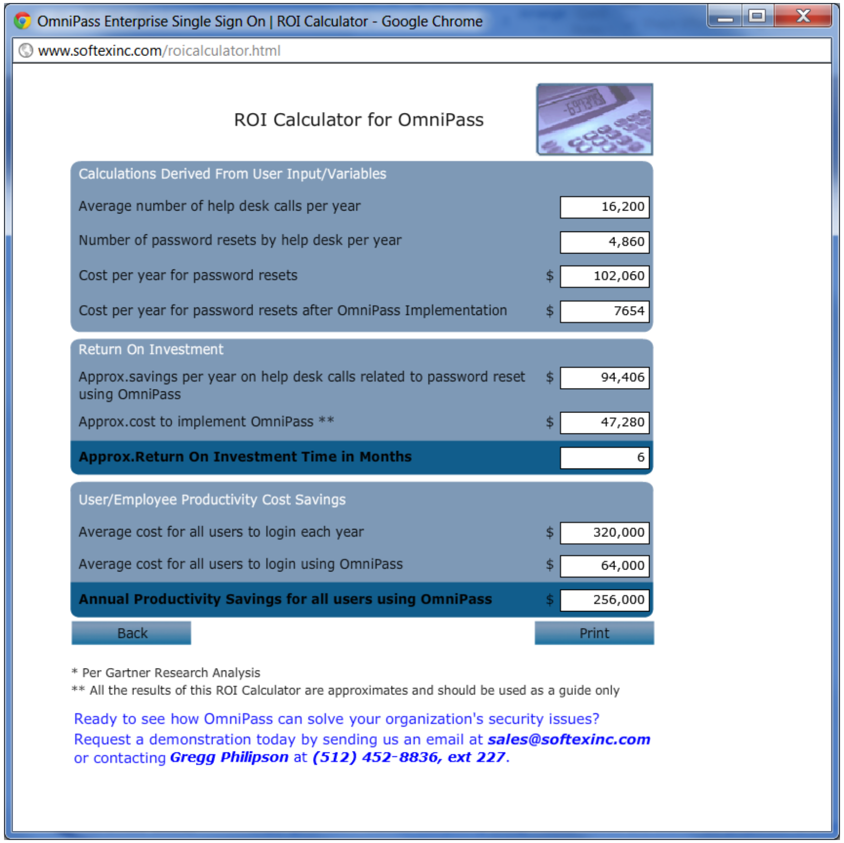
Number of users in your organization to deploy OmniPass		1,000
Number of pc's to deploy OmniPass		1,000
Number of servers to deploy OmniPass		2
Average number of applications user logs in on a daily basis		20
Average time required in seconds to login to the applications		10
Average annual salary of users/employees in the organization	$	50,000

According to Industry Experts (Please change if you have numbers that are more appropriate for your organization)

Average number of I/T help desk calls per user per month*		1.35
% of I/T help desk calls that are related to password resets*	%	30
Average cost per I/T help desk call*	$	21

* Per Gartner Research Analysis
** All the results of this ROI Calculator are approximates and should be used as a guide only

Ready to see how OmniPass can solve your organization's security issues?
Request a demonstration today by sending us an email at ***sales@softexinc.com***
or contacting ***Gregg Philipson*** at ***(512) 452-8836, ext 227***.


OmniPass Enterprise Single Sign On | ROI Calculator - Google Chrome
www.softexinc.com/roicalculator.html

ROI Calculator for OmniPass

Calculations Derived From User Input/Variables

Average number of help desk calls per year		16,200
Number of password resets by help desk per year		4,860
Cost per year for password resets	$	102,060
Cost per year for password resets after OmniPass Implementation	$	7654

Return On Investment

Approx.savings per year on help desk calls related to password reset using OmniPass	$	94,406
Approx.cost to implement OmniPass **	$	47,280
Approx.Return On Investment Time in Months		6

User/Employee Productivity Cost Savings

Average cost for all users to login each year	$	320,000
Average cost for all users to login using OmniPass	$	64,000
Annual Productivity Savings for all users using OmniPass	$	256,000

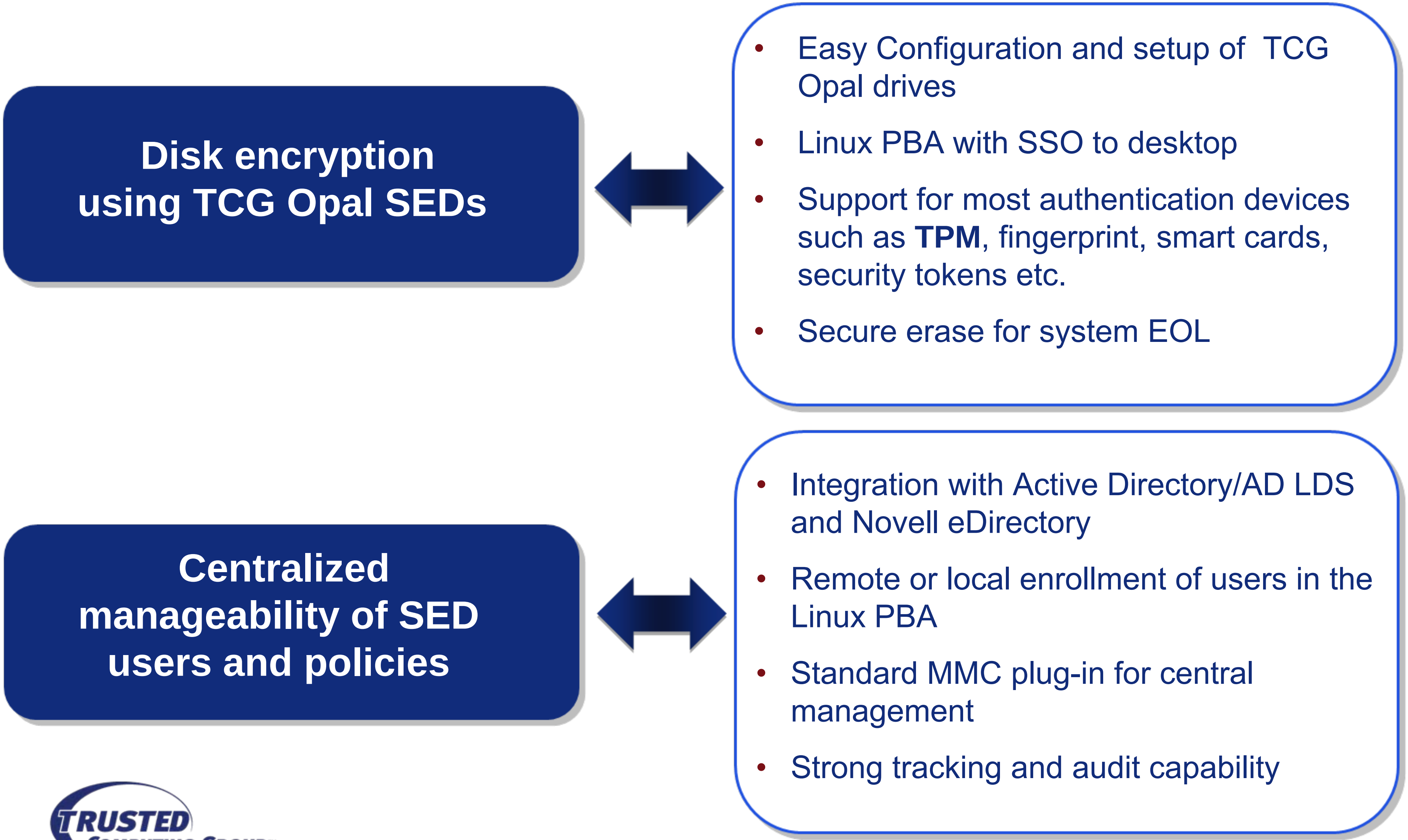
* Per Gartner Research Analysis
** All the results of this ROI Calculator are approximates and should be used as a guide only

Ready to see how OmniPass can solve your organization's security issues?
Request a demonstration today by sending us an email at ***sales@softexinc.com***
or contacting ***Gregg Philipson*** at ***(512) 452-8836, ext 227***.

Click here to calculate the ROI for your organization

http://www.softexinc.com/roicalculator.html

SecureDrive Overview



Disk encryption using TCG Opal SEDs

- Easy Configuration and setup of TCG Opal drives
- Linux PBA with SSO to desktop
- Support for most authentication devices such as **TPM**, fingerprint, smart cards, security tokens etc.
- Secure erase for system EOL

Centralized manageability of SED users and policies

- Integration with Active Directory/AD LDS and Novell eDirectory
- Remote or local enrollment of users in the Linux PBA
- Standard MMC plug-in for central management
- Strong tracking and audit capability

Resources

To View This or Other Events On-Demand Please Visit:

http://www.netseminar.com

For more information on the Trusted Computing Group, please visit:

Technical

http://www.trustedcomputinggroup.org/developers/trusted_platform_module

Business

http://www.trustedcomputinggroup.org/solutions/authentication