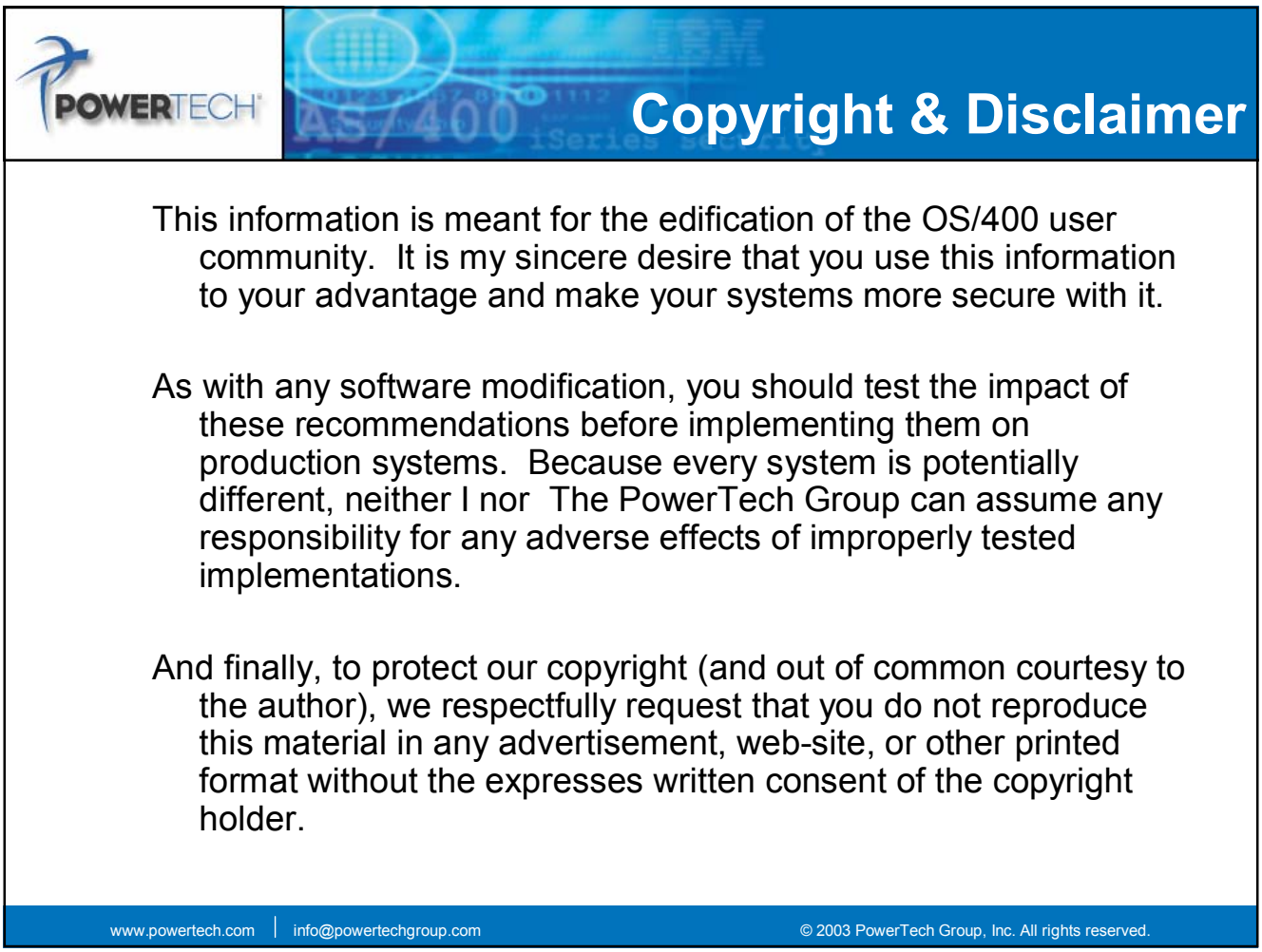
A PRESENTATION

Top 10 OS/400 Security Risks

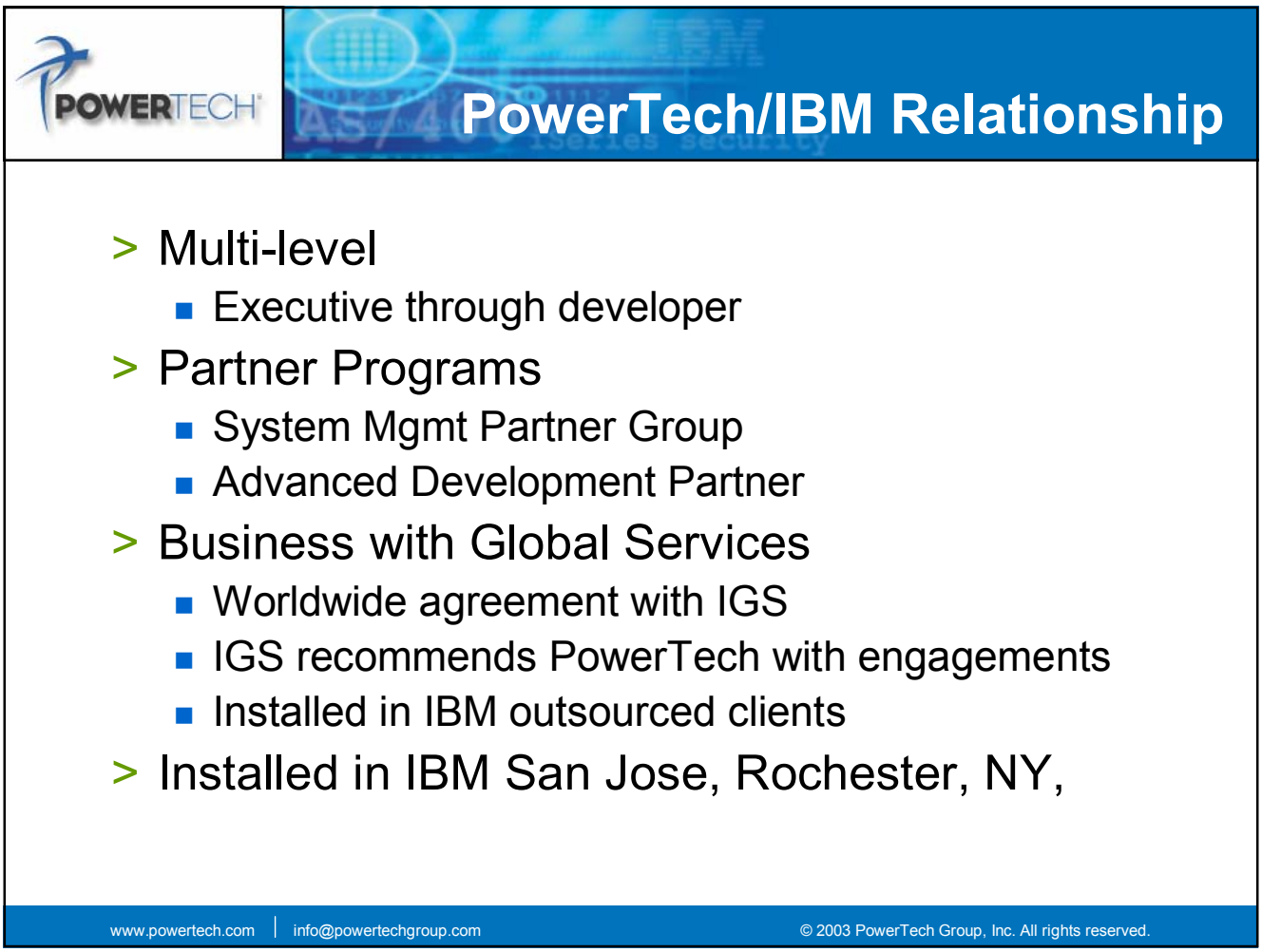
October 2004

John Earl
Chief Technology Officer
The PowerTech Group
www. powertech.com
john.earl@ powertech.com

opyright (c) 1999 - 2002 The Powertech



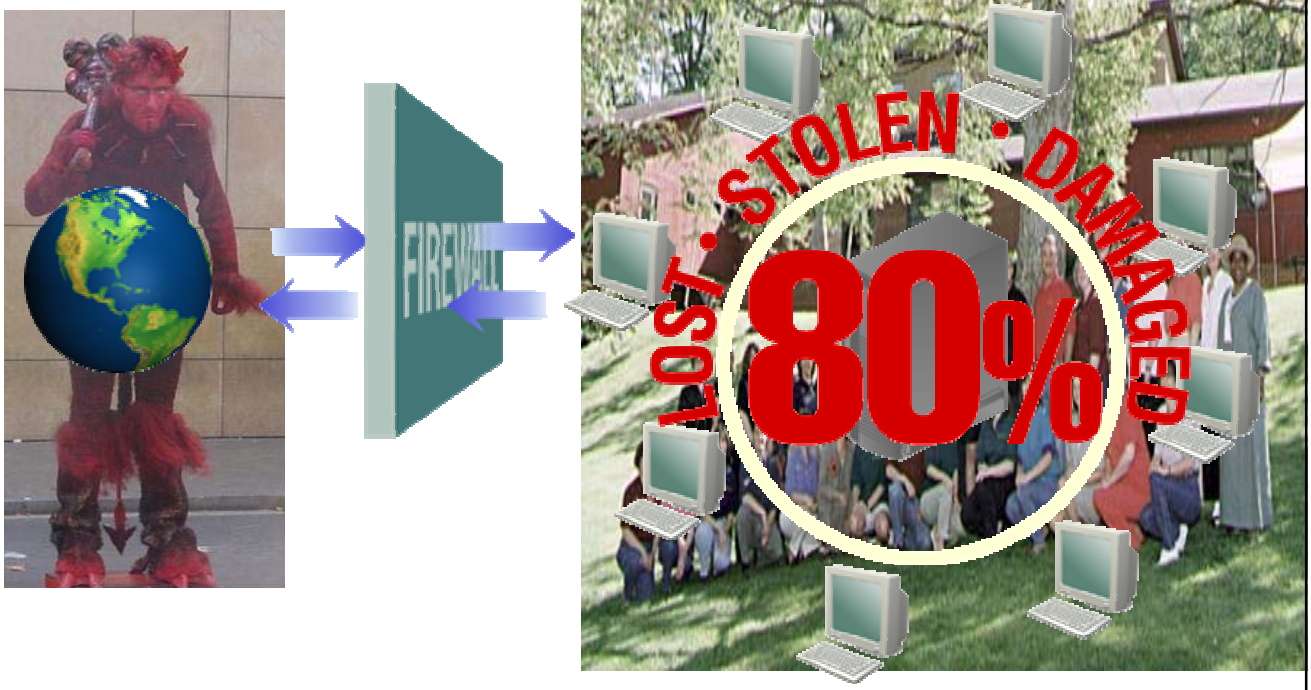
opyright (c) 1999 - 2002 The Powertech



opyright (c) 1999 - 2002 The Powertech

The Biggest Threat to your Corporate Data

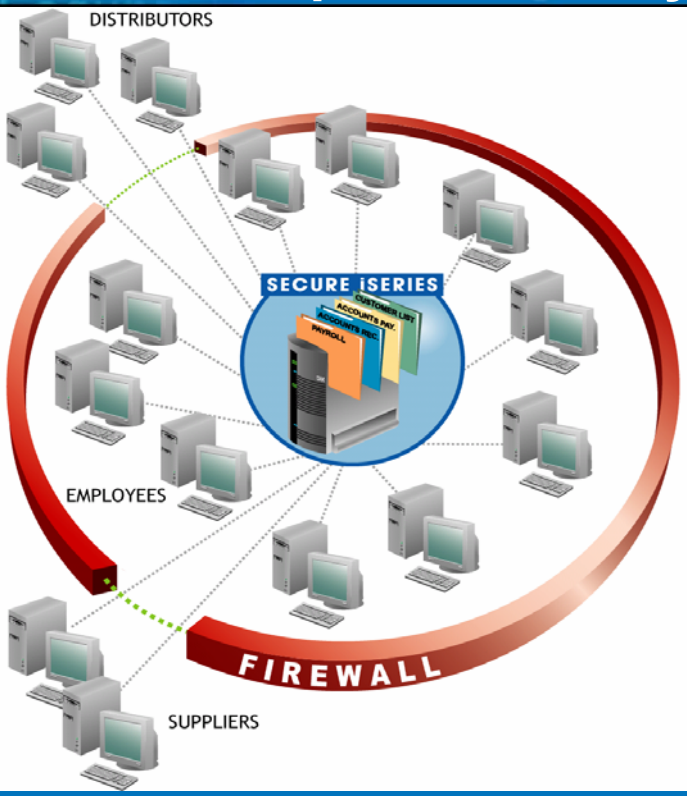
HACKERS!!! or Your Company



© 2003 PowerTech Group, Inc. All rights reserved.

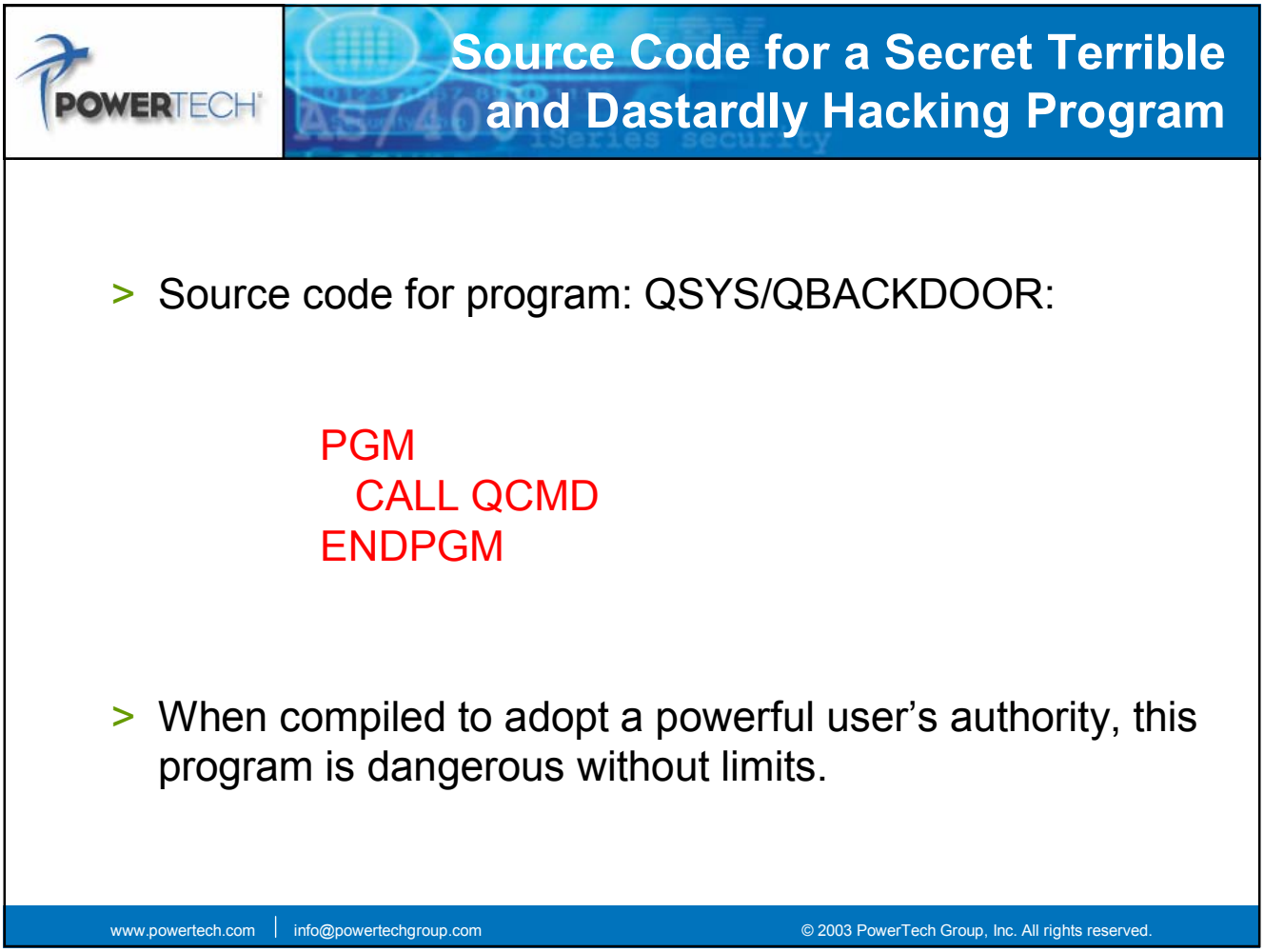
opyright (c) 1999 - 2002 The Powertech

Enterprise Security Evolution



© 2003 PowerTech Group, Inc. All rights reserved.

opyright (c) 1999 - 2002 The Powertech



opyright (c) 1999 - 2002 The Powertech

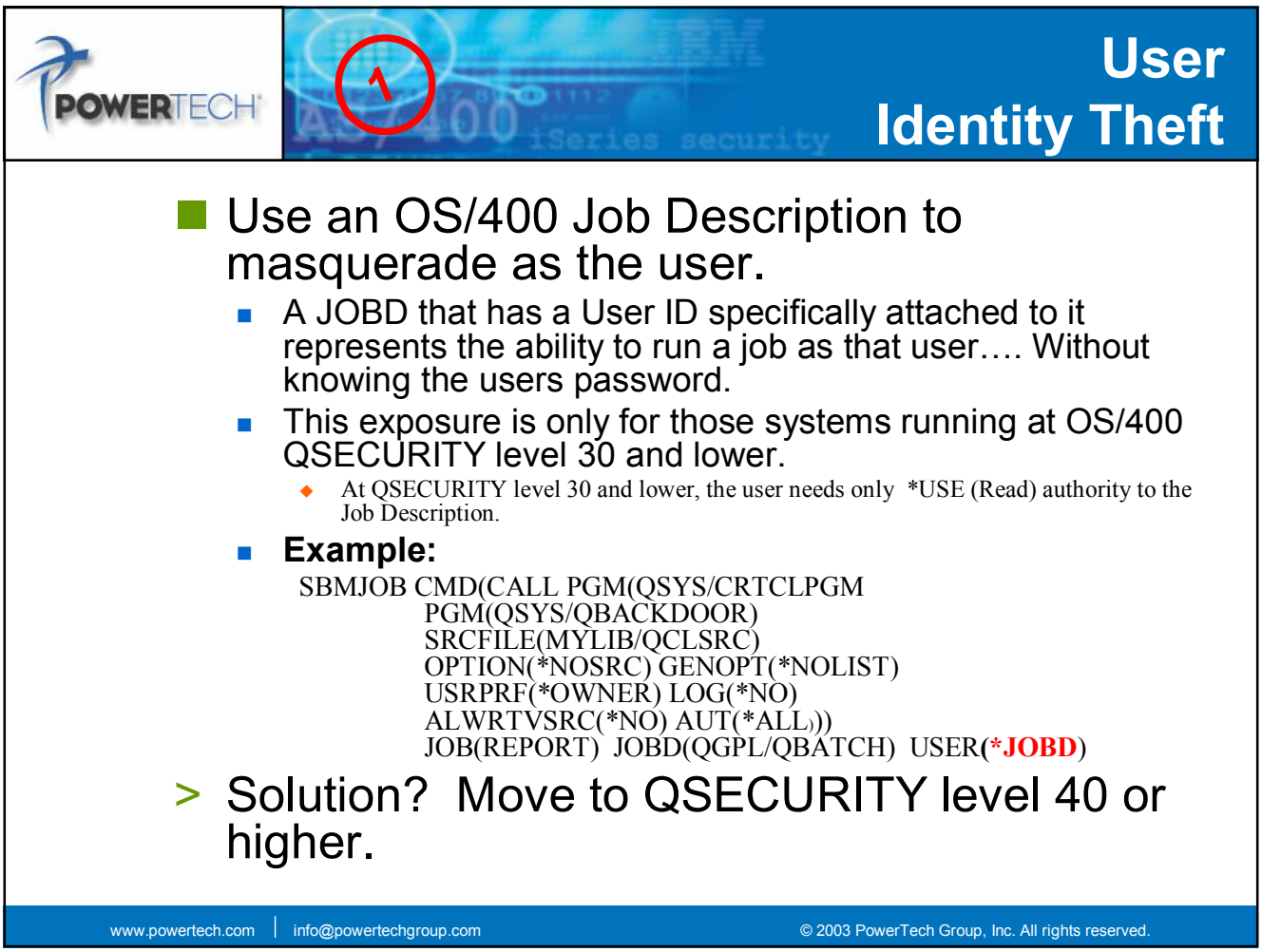
opyright (c) 1999 - 2002 The Powertech

User Identity Theft

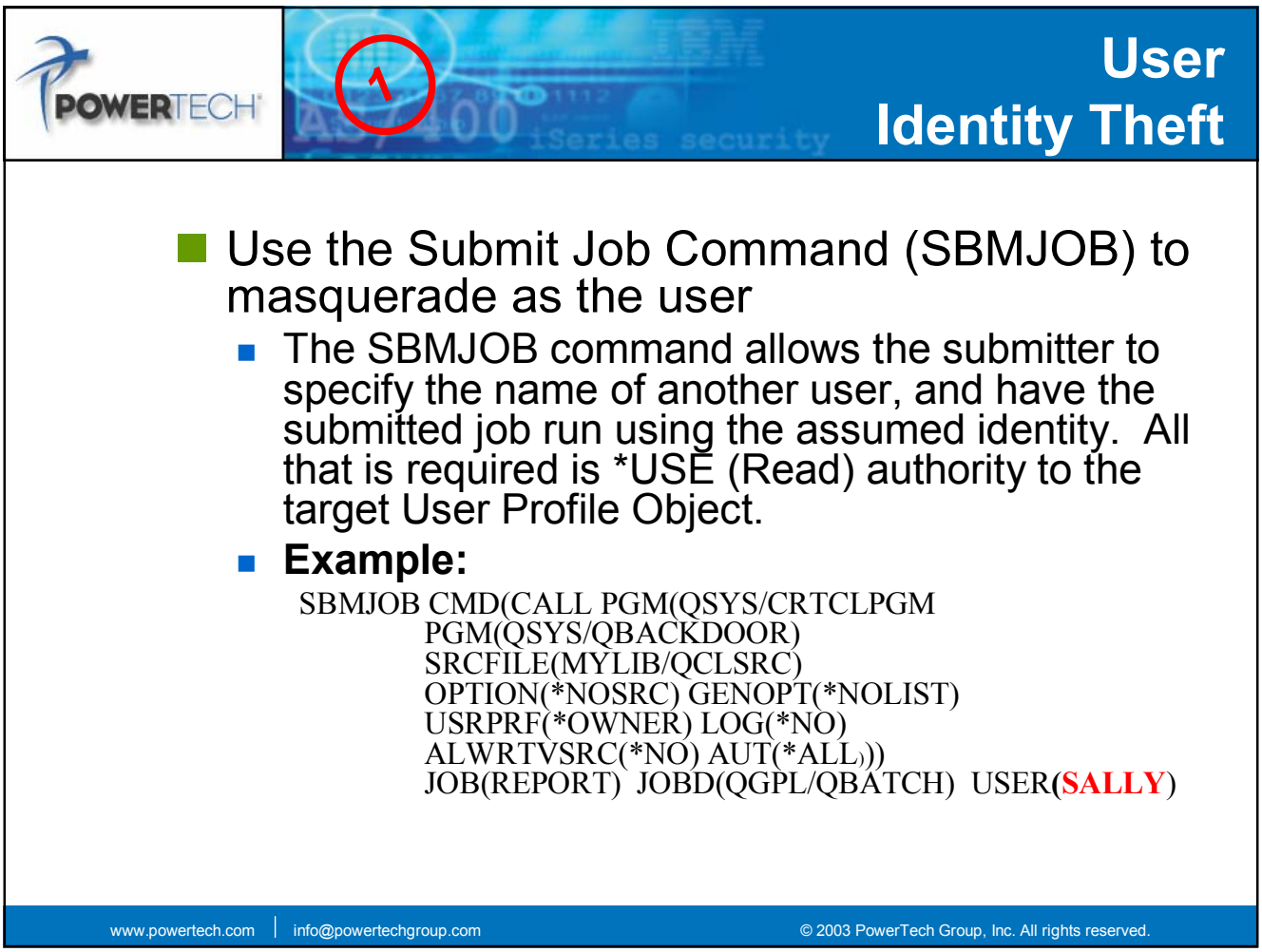
- There are 5 well known ways to steal an OS/400 User IDs.
  - From the difficult to the easy, they are:
    1. Use an OS/400 Job Description to masquerade as the user
    2. Use the Submit Job Command (SBMJOB) to masquerade as the user
    3. Use IBM API's to Switch to the user (no password required)
    4. Sniff Network traffic to find clear text passwords
    5. Beg, borrow, steal or guess their password

© 2003 PowerTech Group, Inc. All rights reserved.

opyright (c) 1999 - 2002 The Powertech



opyright (c) 1999 - 2002 The Powertech



opyright (c) 1999 - 2002 The Powertech

User Identity Theft

- Use IBM API's to Switch to the user (no password required)
  - The following code will allow me to become someone else without knowing their password.
    - Program QSYS/QASSUME

```
PGM  PARM(&USER)
     DCL      &USER
     DCL      &HANDLE
     DCL      &ERROR
     CHGVAR %
     CALL                                                +
                                    &HANDLE &ERROR)
     CH                             0
     CAL                            ARM(&HANDLE &ERROR)
ENDPGM
```

© 2003 PowerTech Group, Inc. All rights reserved.

opyright (c) 1999 - 2002 The Powertech

User Identity Theft

- Sniff Network traffic to find clear text passwords
  - Several Protocols submit User ID's and Passwords in clear text
    - Among them are FTP, Telnet, and older forms of Client Access and PC Support
  - Minimize use of the legacy OS/400 Sign-on Screen (QDSIGNON)
  - Set the Client Access "Bypass Signon" flag to yes, and the OS/400 system value for QRMTSIGN to "*VERIFY"
  - Use VPN's when communicating over un-secure networks

© 2003 PowerTech Group, Inc. All rights reserved.

opyright (c) 1999 - 2002 The Powertech

- Beg, borrow, steal, or guess their password.
  - Password Protection is the Best Defense!
    - AS/400 requires a password to in order to access
    - A solid password policy will prevent most breaches from the outside – and from nefarious insiders too.
    - Don't send passwords via email, or over un-secured networks.
    - Require that passwords be changed at regular intervals.
    - Don't **EVER** use default passwords

© 2003 PowerTech Group, Inc. All rights reserved.

opyright (c) 1999 - 2002 The Powertech

All of the Default passwords are well known!

Subject: alt.2600 FAQ (1/3) #18/
From: quinny@bigfoot.com
Forums: alt.2600
Message segment 18 of 63 - Get Previous / Next Segment - Get All 63 Segments

AS/400
~~~~~~

```
qsecofr     qsecofr     /* master security officer */
qsysopr     qsysopr     /* system operator         */
qpgmr       qpgmr       /* default programmer      */
ibm         password
ibm         2222
ibm         service
qsecofr     1111111
qsecofr     2222222
qserv       qserv
qsvr        qsvr
secofr      secofr
qsrv        ibmce
```

(Get All 63 Segments)

© 2003 PowerTech Group, Inc. All rights reserved.

opyright (c) 1999 - 2002 The Powertech
~~~~~~

User Identity Theft

Prevent Trivial Passwords:

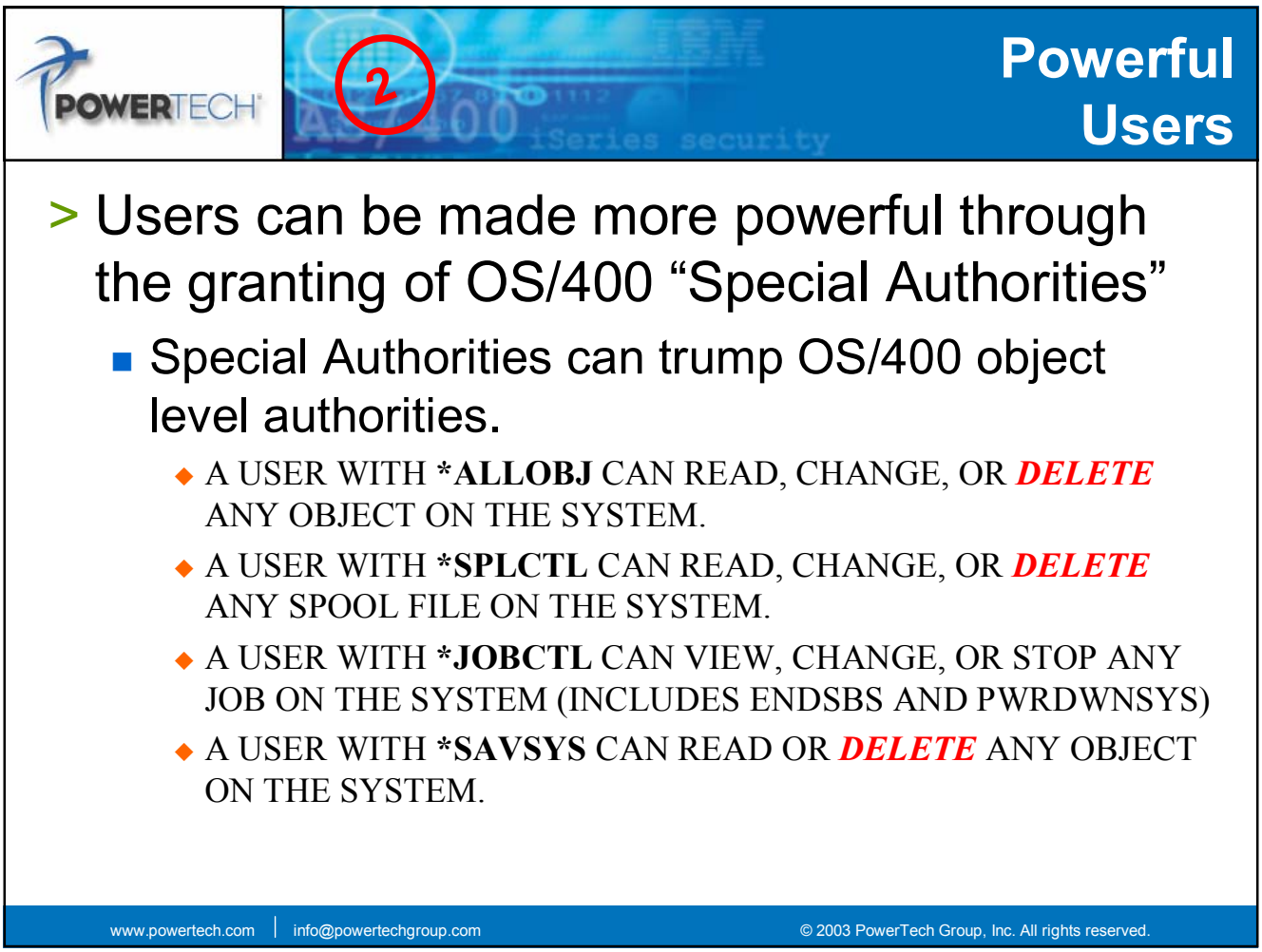
- **At a minimum, set these system values:**

System Value Name	Value	Description
QPWDEXPITV	90	90 Days
QPWDMINLEN	6	6 Character Minimum length
QPWDRQDDGT	1	Require a digit
QPWDRQDDIF	5	Unique in 10

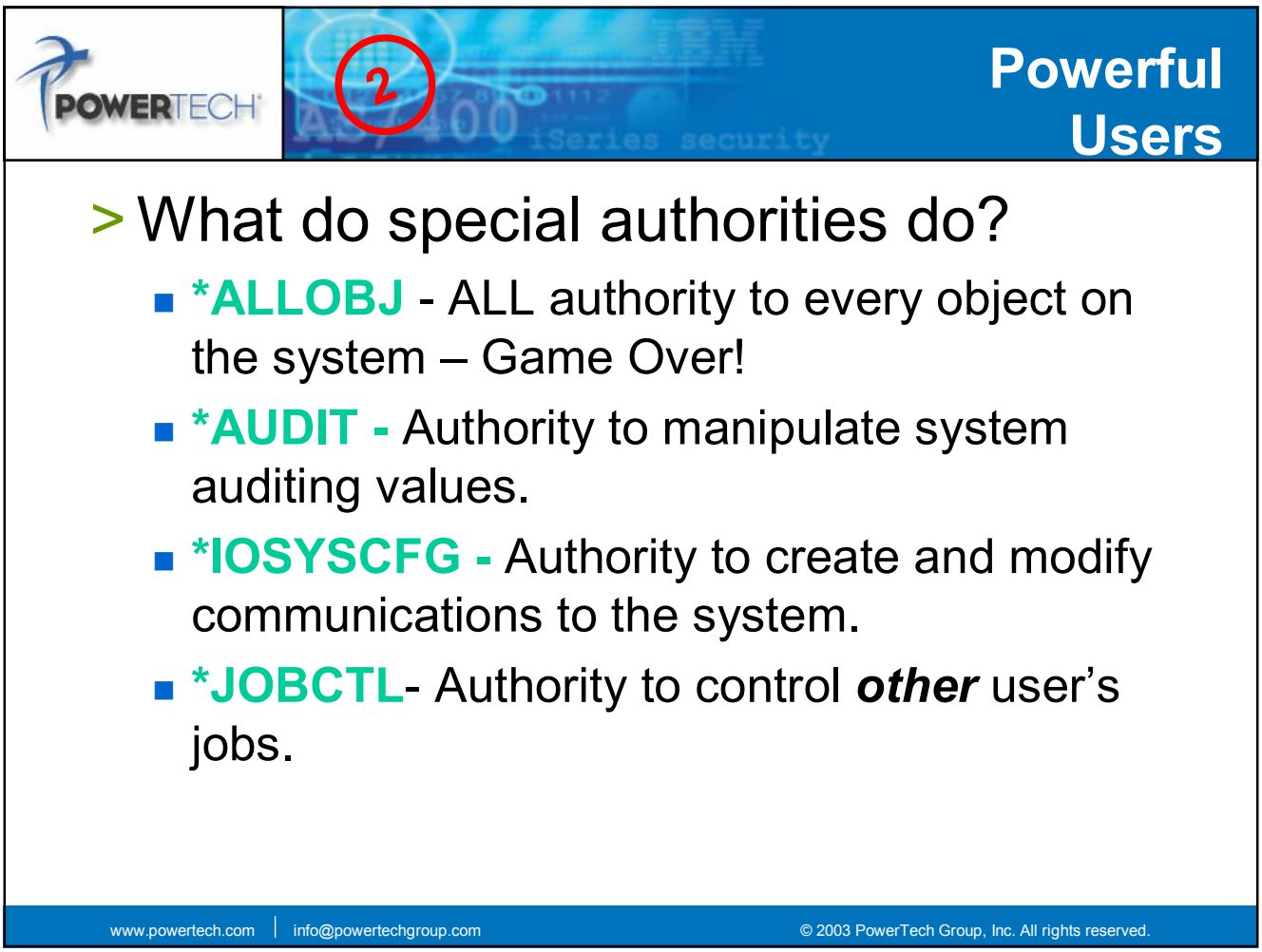
- Don't go too wild with password rules (the QPWD* system values), or your users won't remember their passwords!

© 2003 PowerTech Group, Inc. All rights reserved.

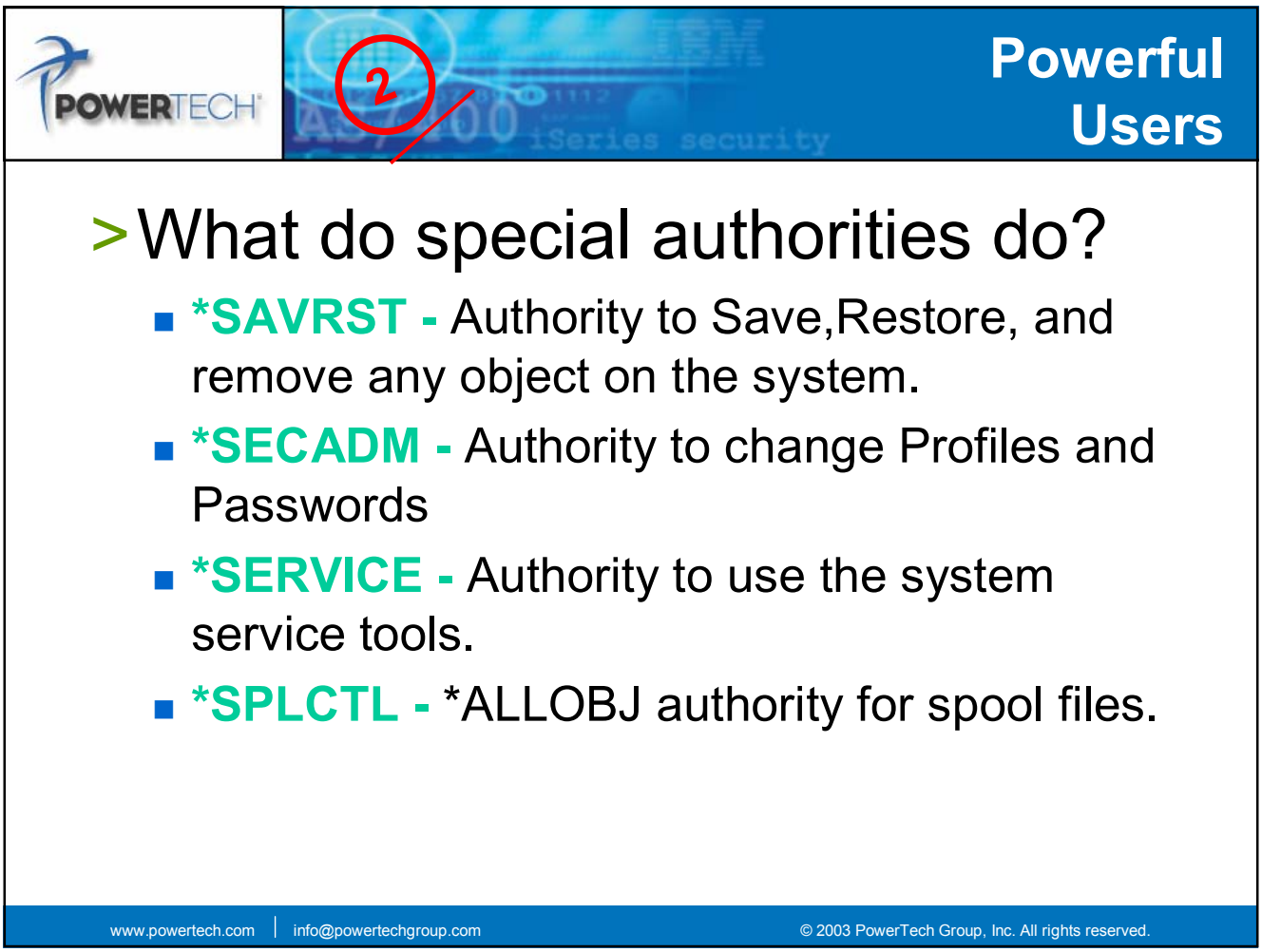
opyright (c) 1999 - 2002 The Powertech



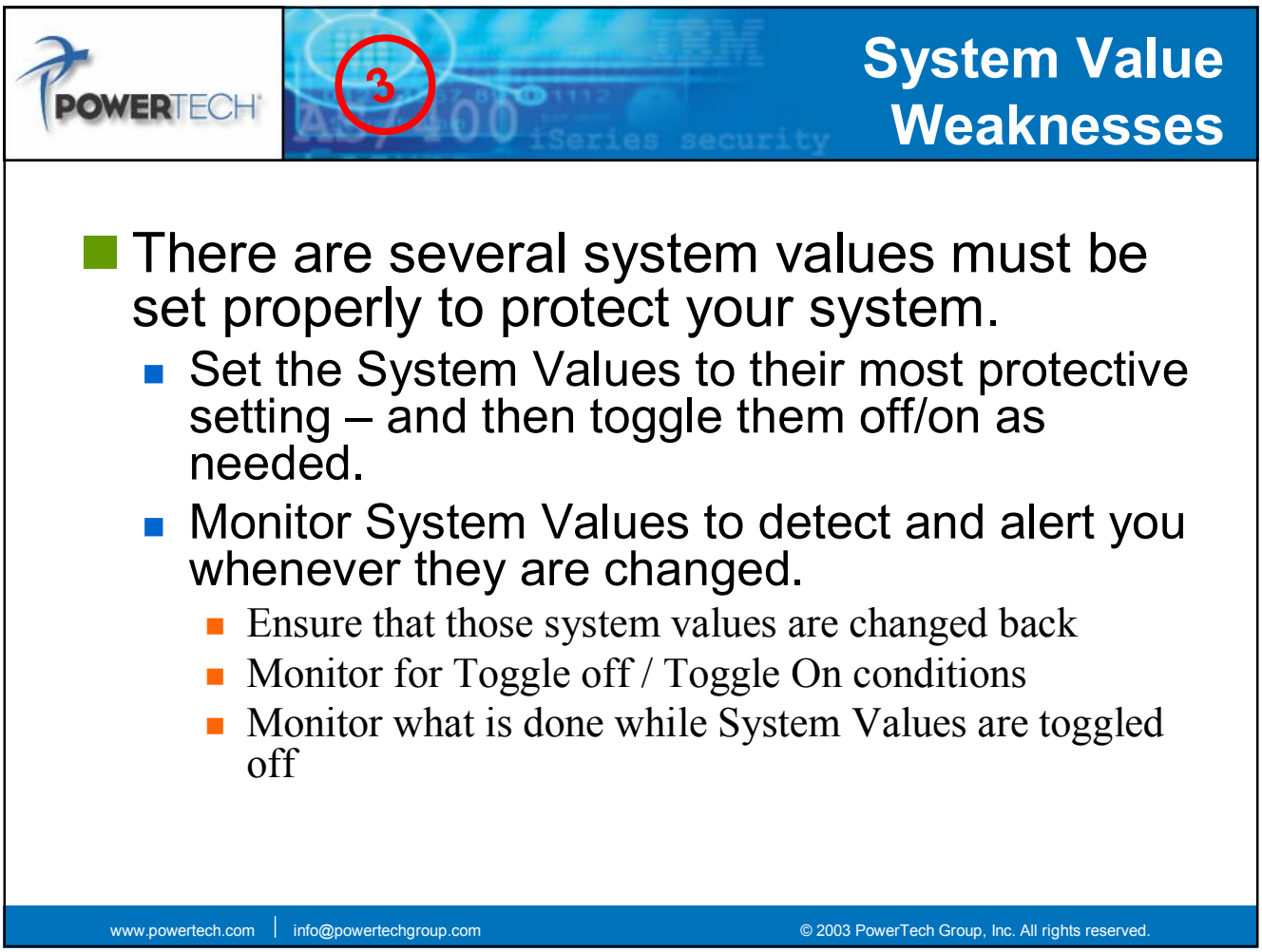
opyright (c) 1999 - 2002 The Powertech



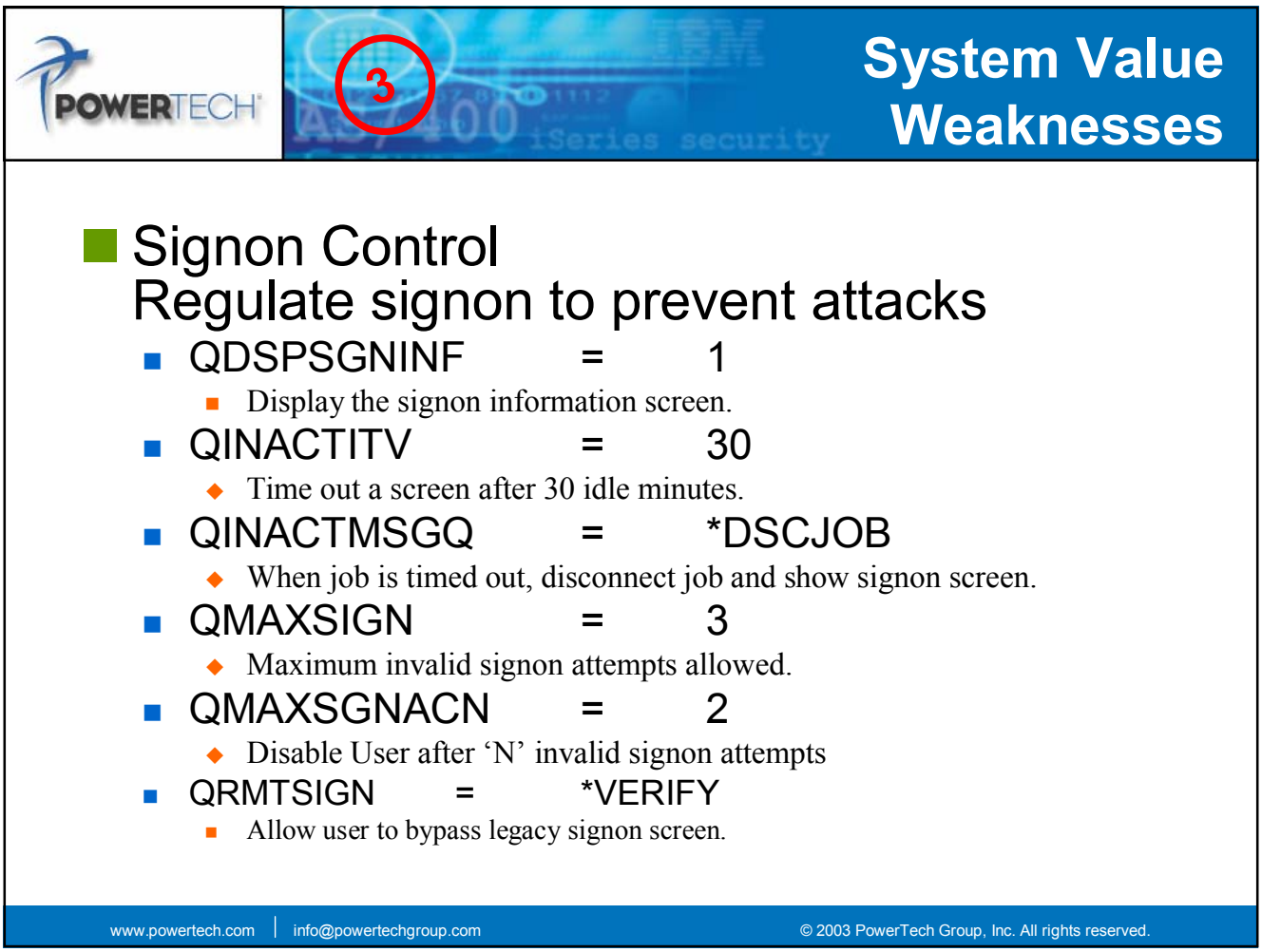
opyright (c) 1999 - 2002 The Powertech



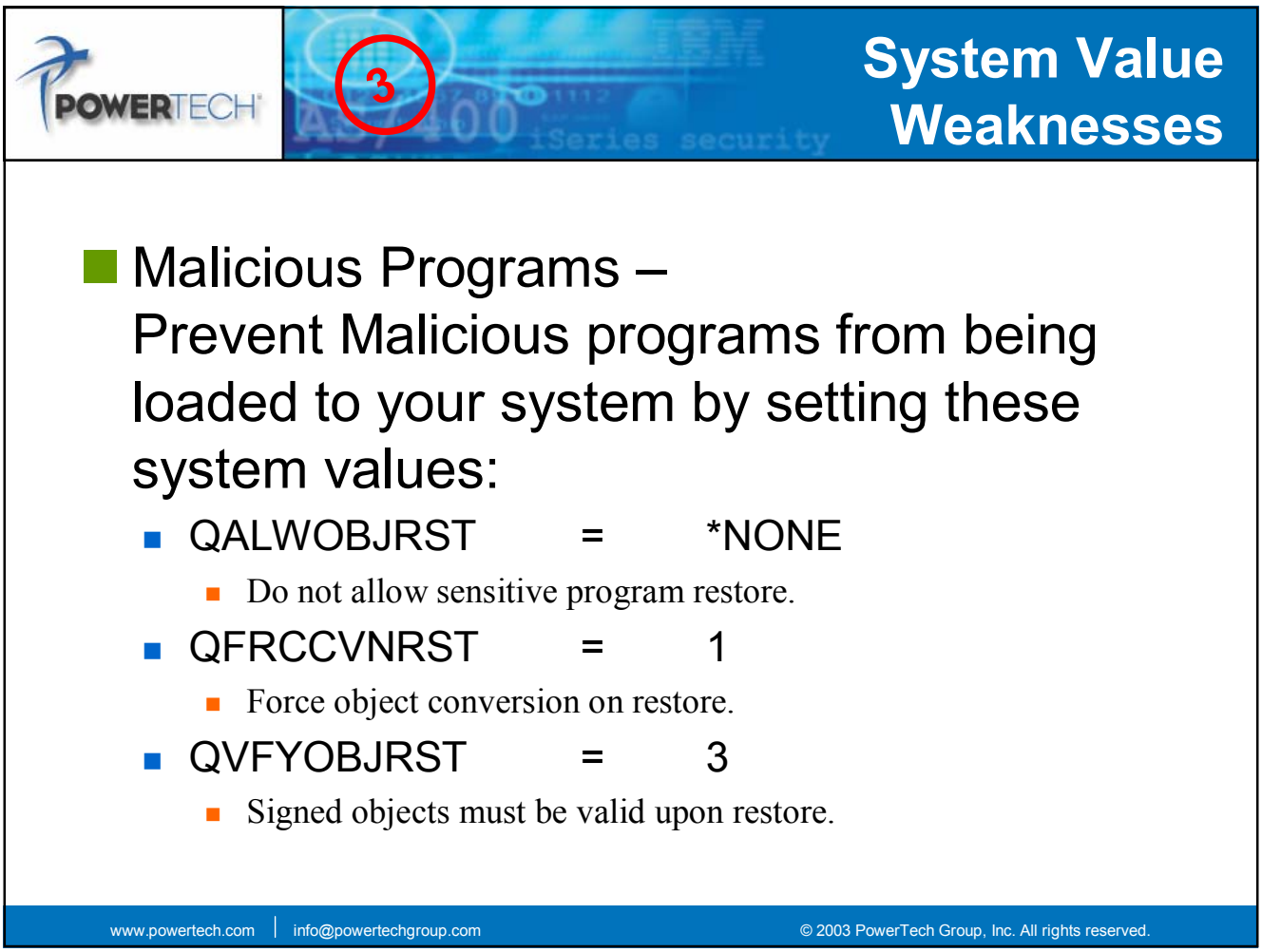
opyright (c) 1999 - 2002 The Powertech



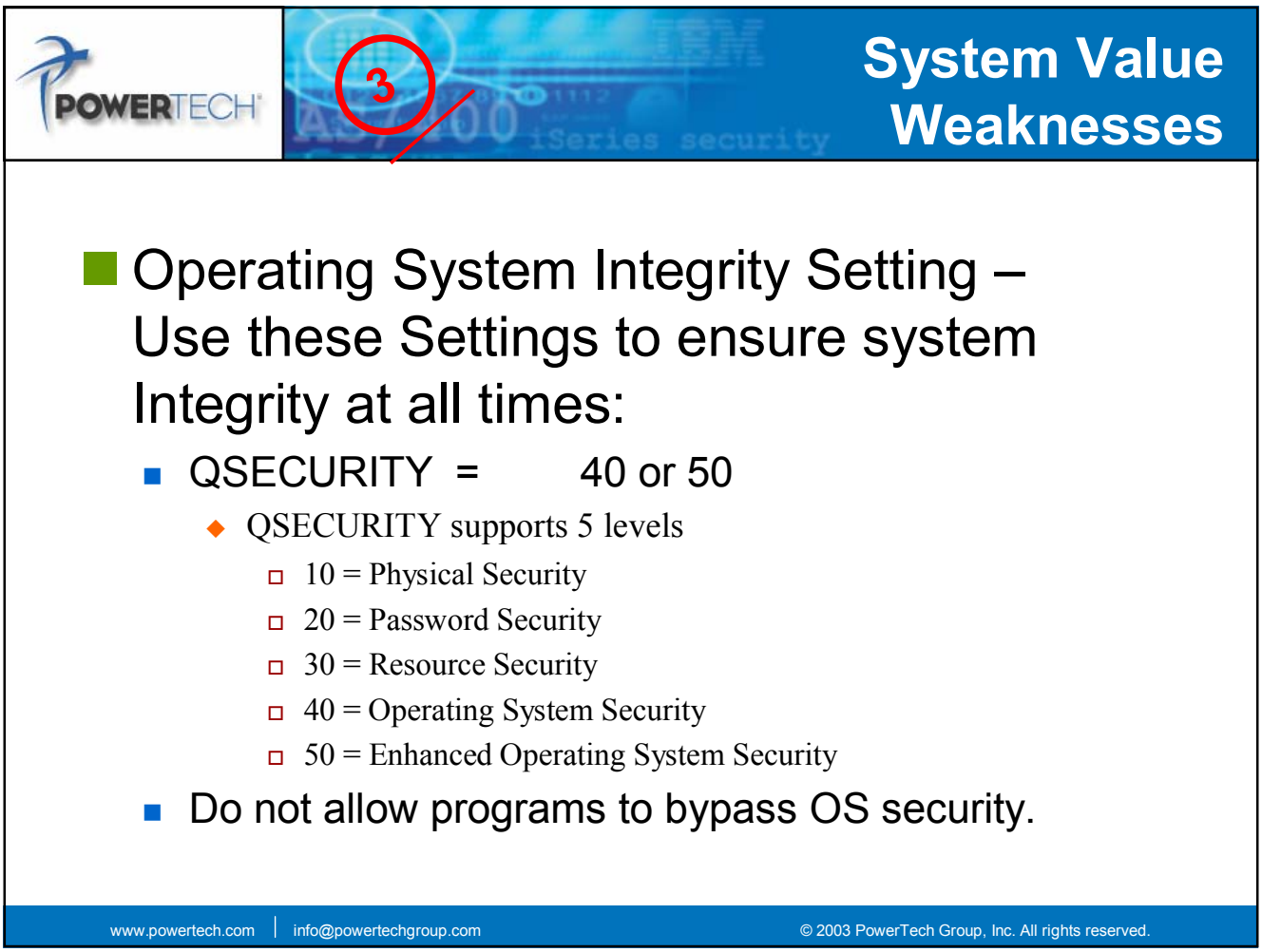
opyright (c) 1999 - 2002 The Powertech



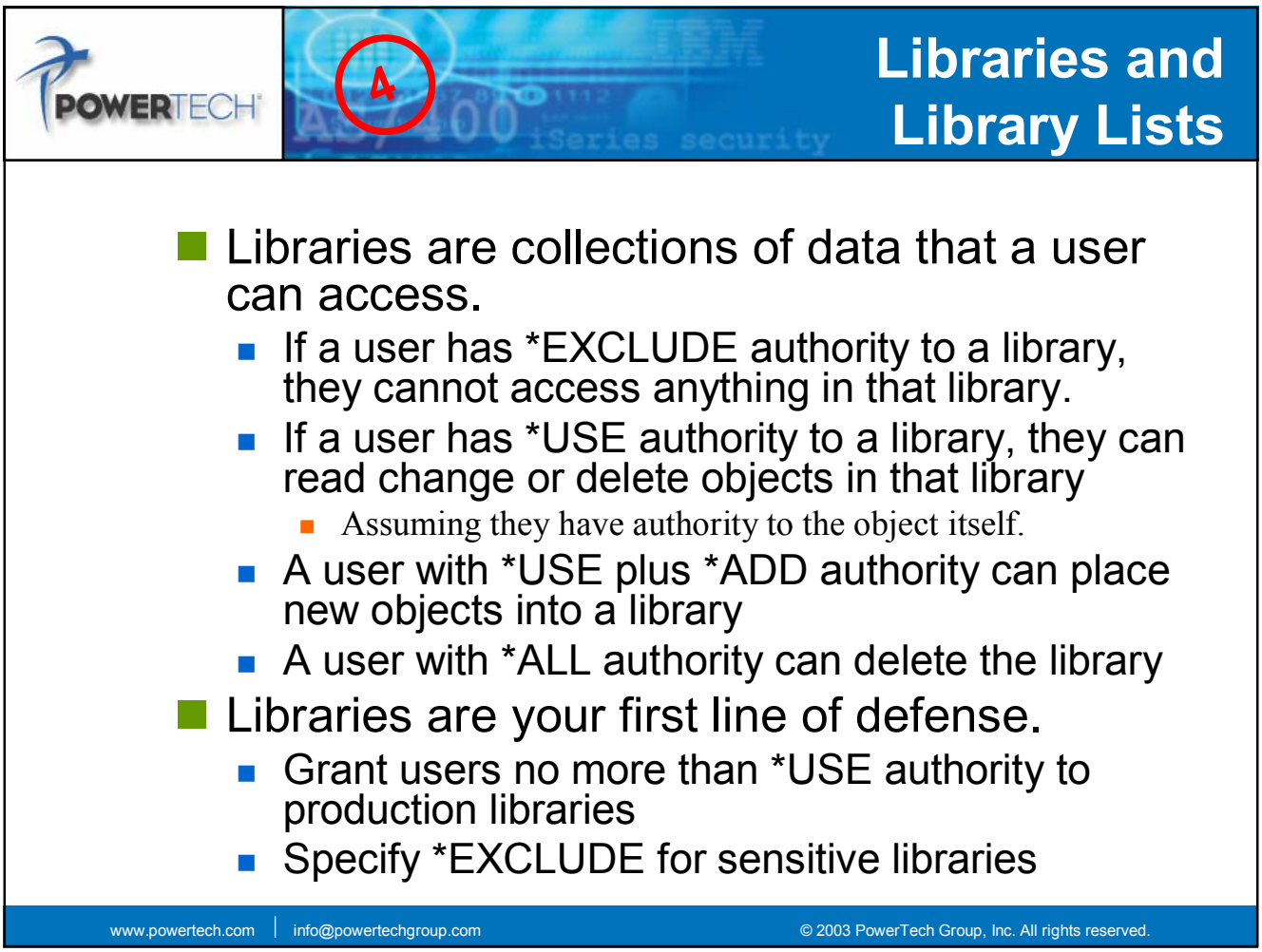
opyright (c) 1999 - 2002 The Powertech



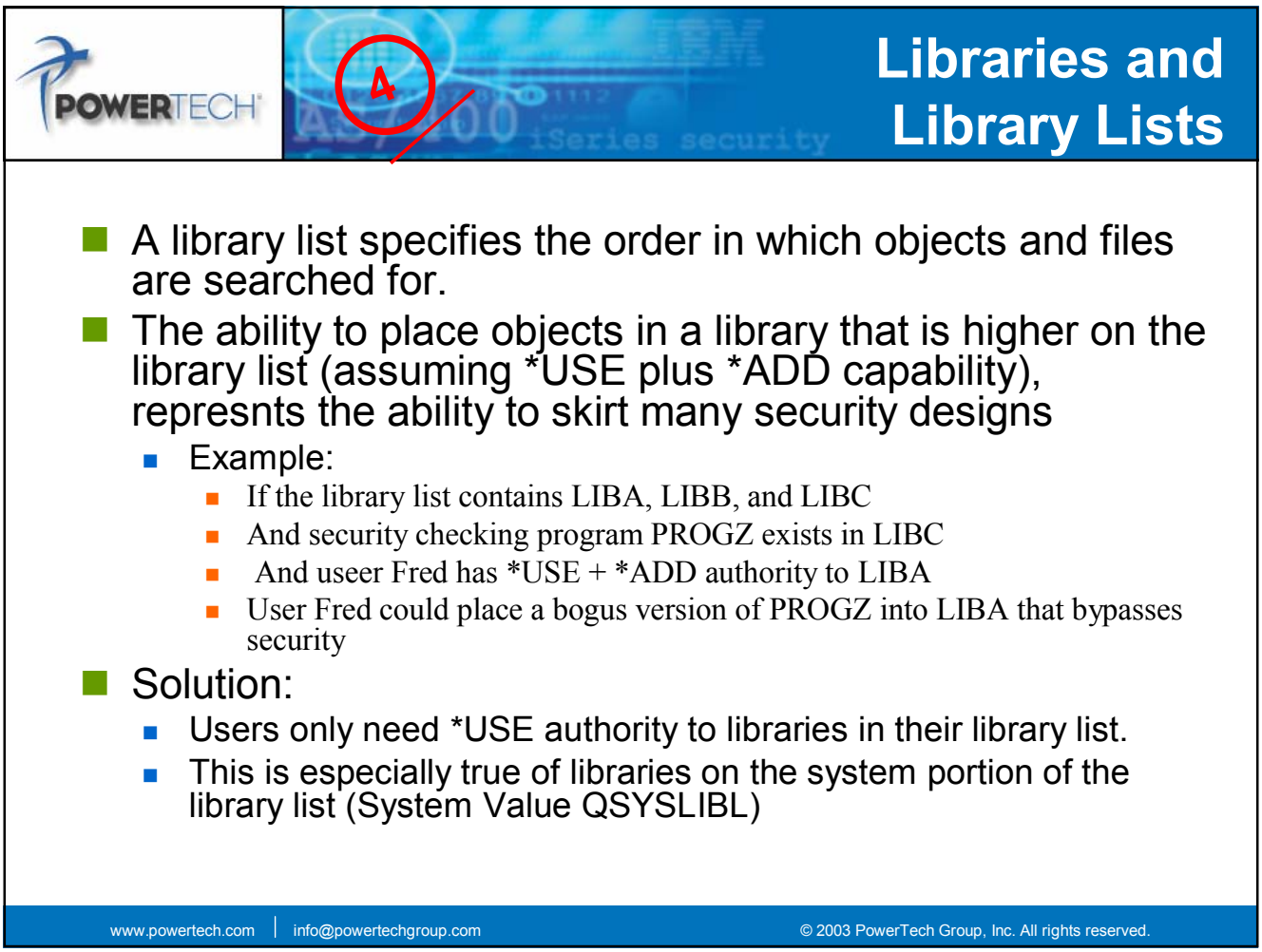
opyright (c) 1999 - 2002 The Powertech



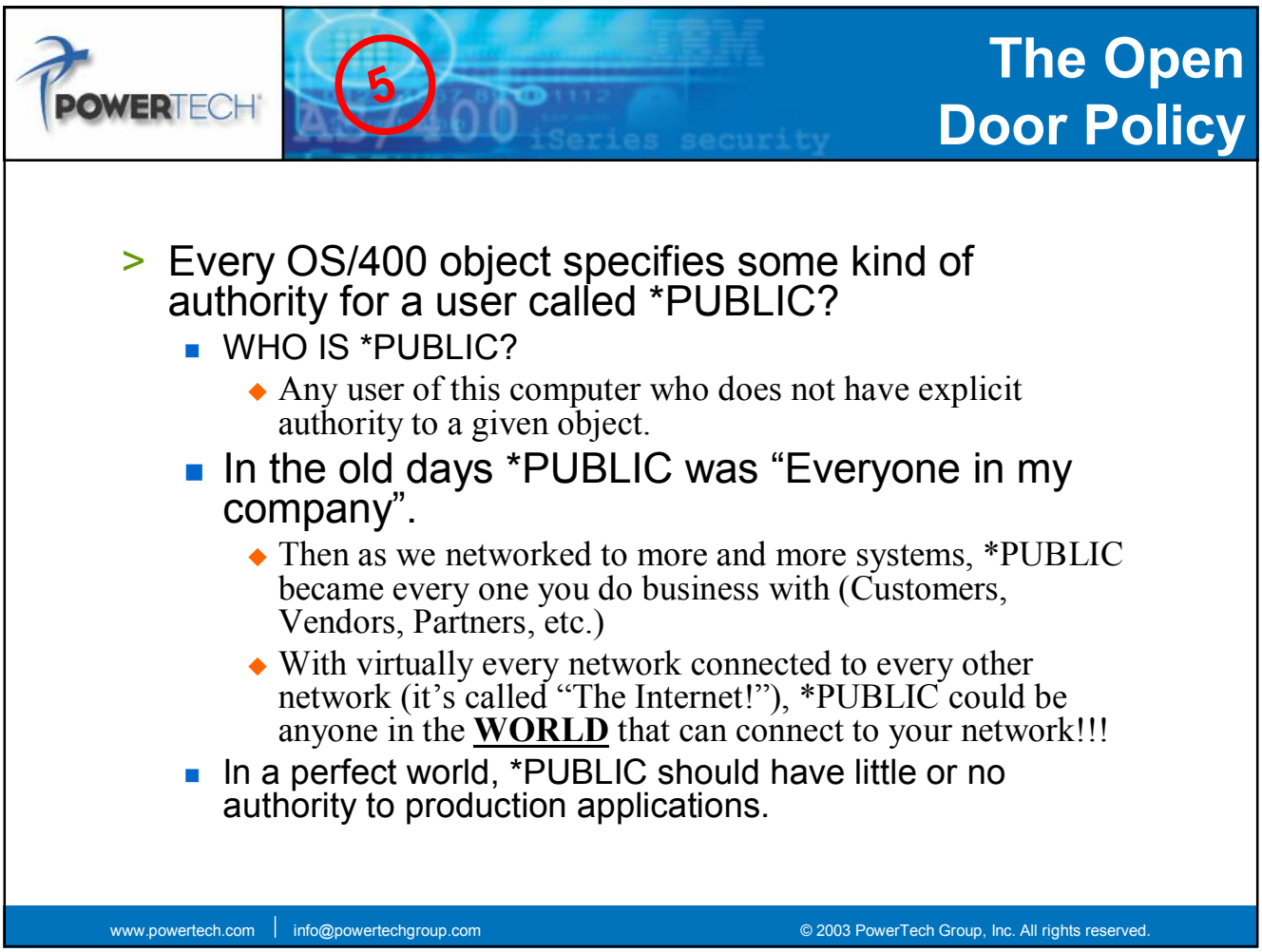
opyright (c) 1999 - 2002 The Powertech



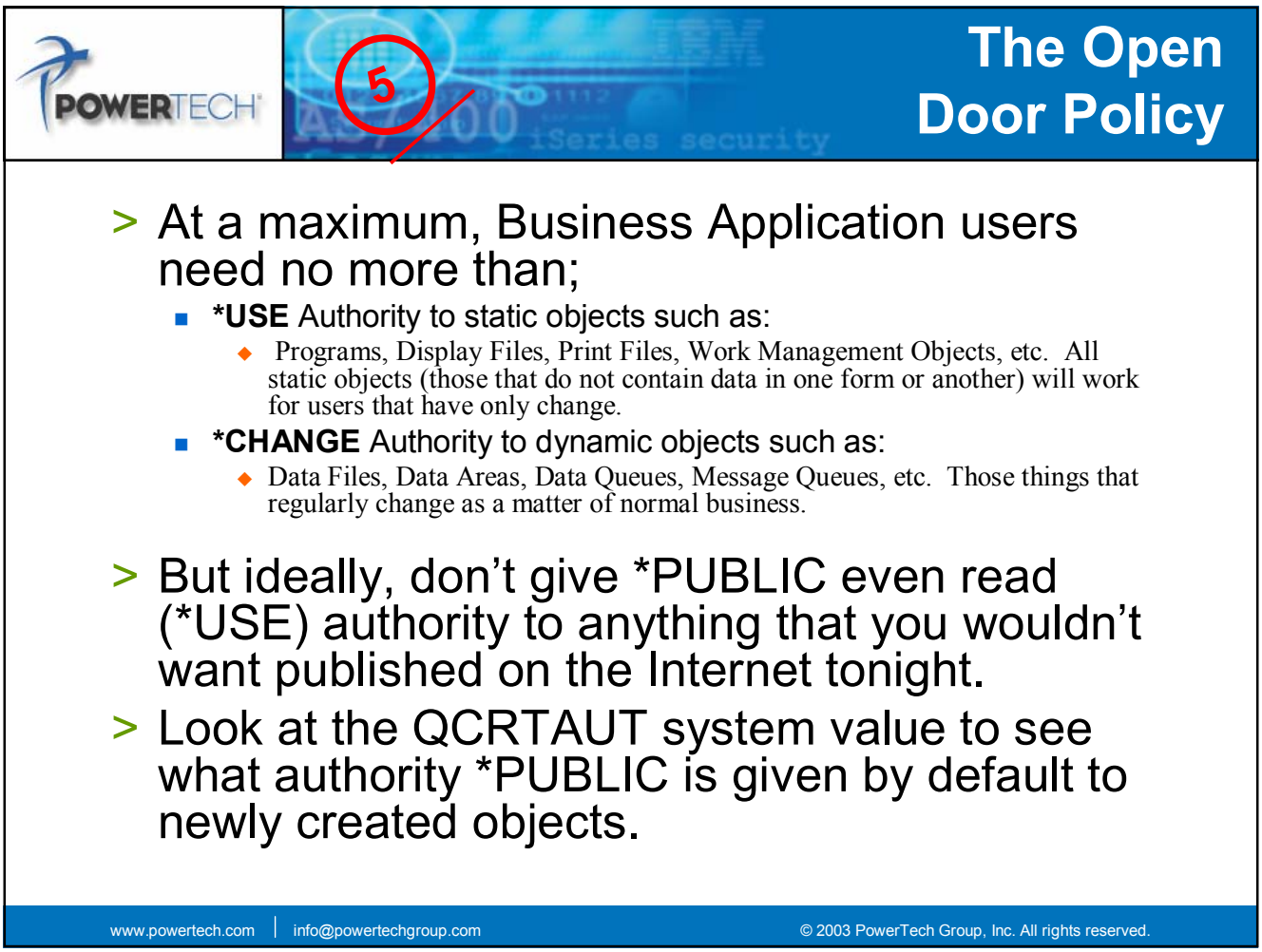
opyright (c) 1999 - 2002 The Powertech



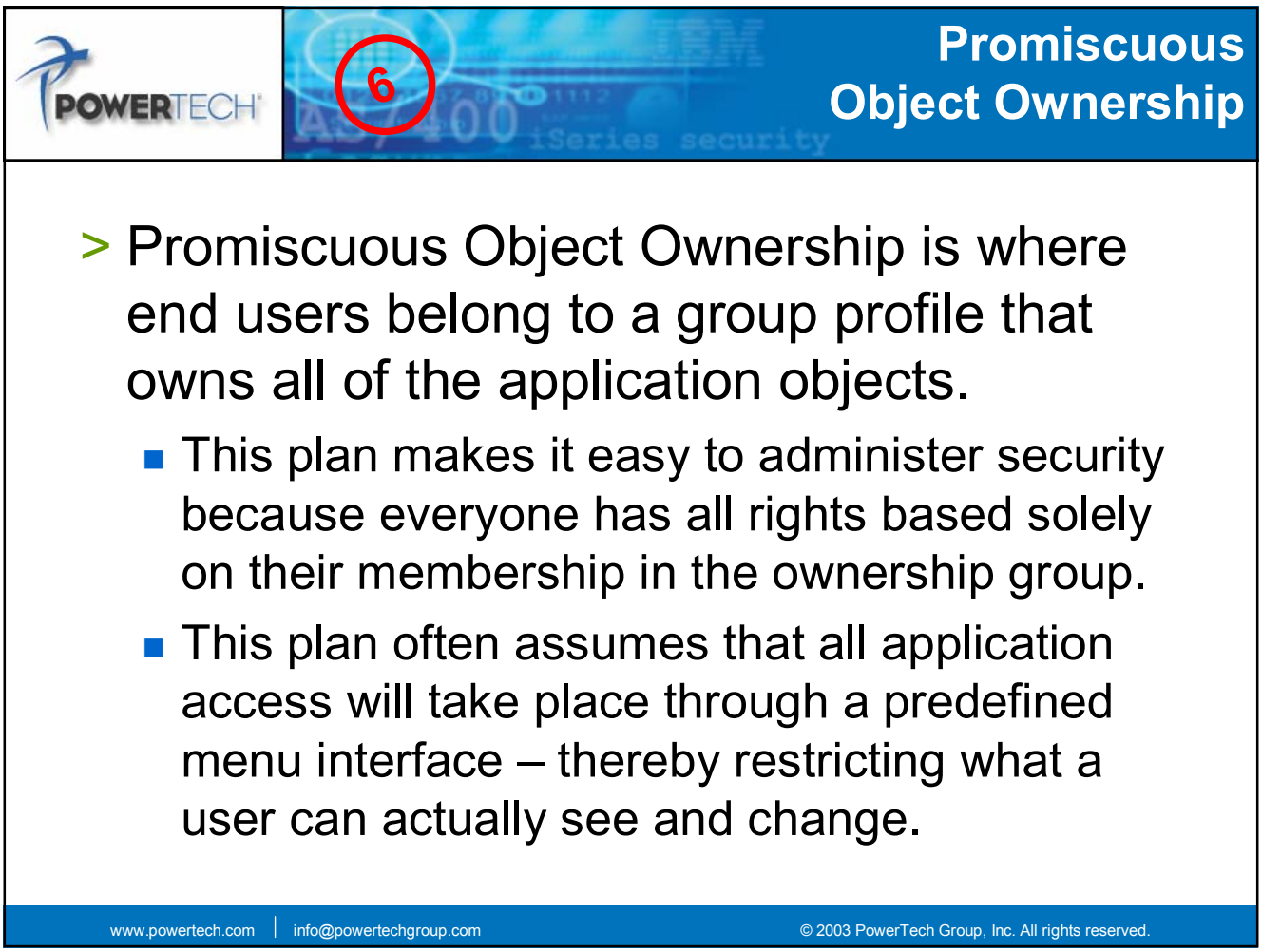
opyright (c) 1999 - 2002 The Powertech



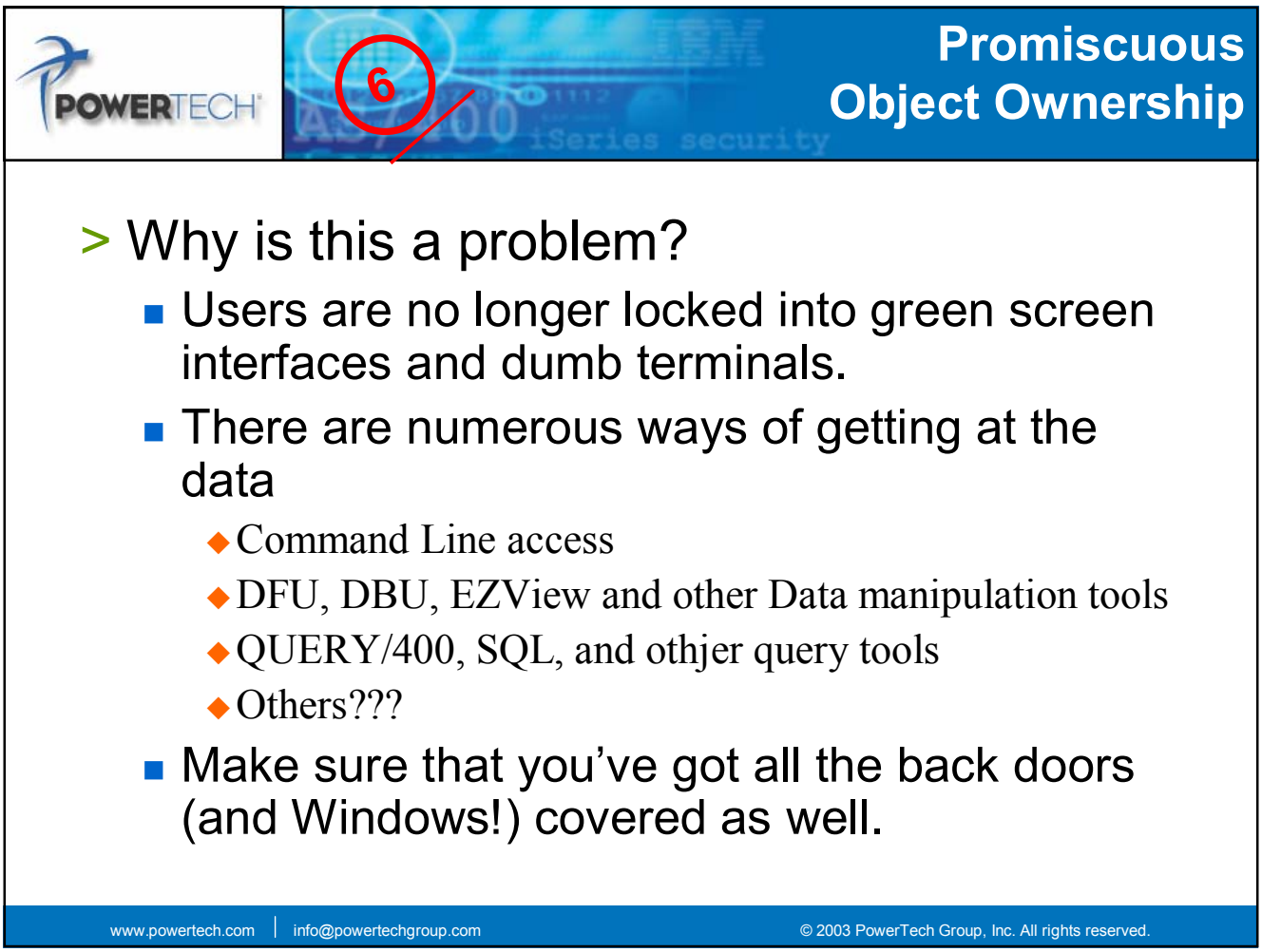
opyright (c) 1999 - 2002 The Powertech



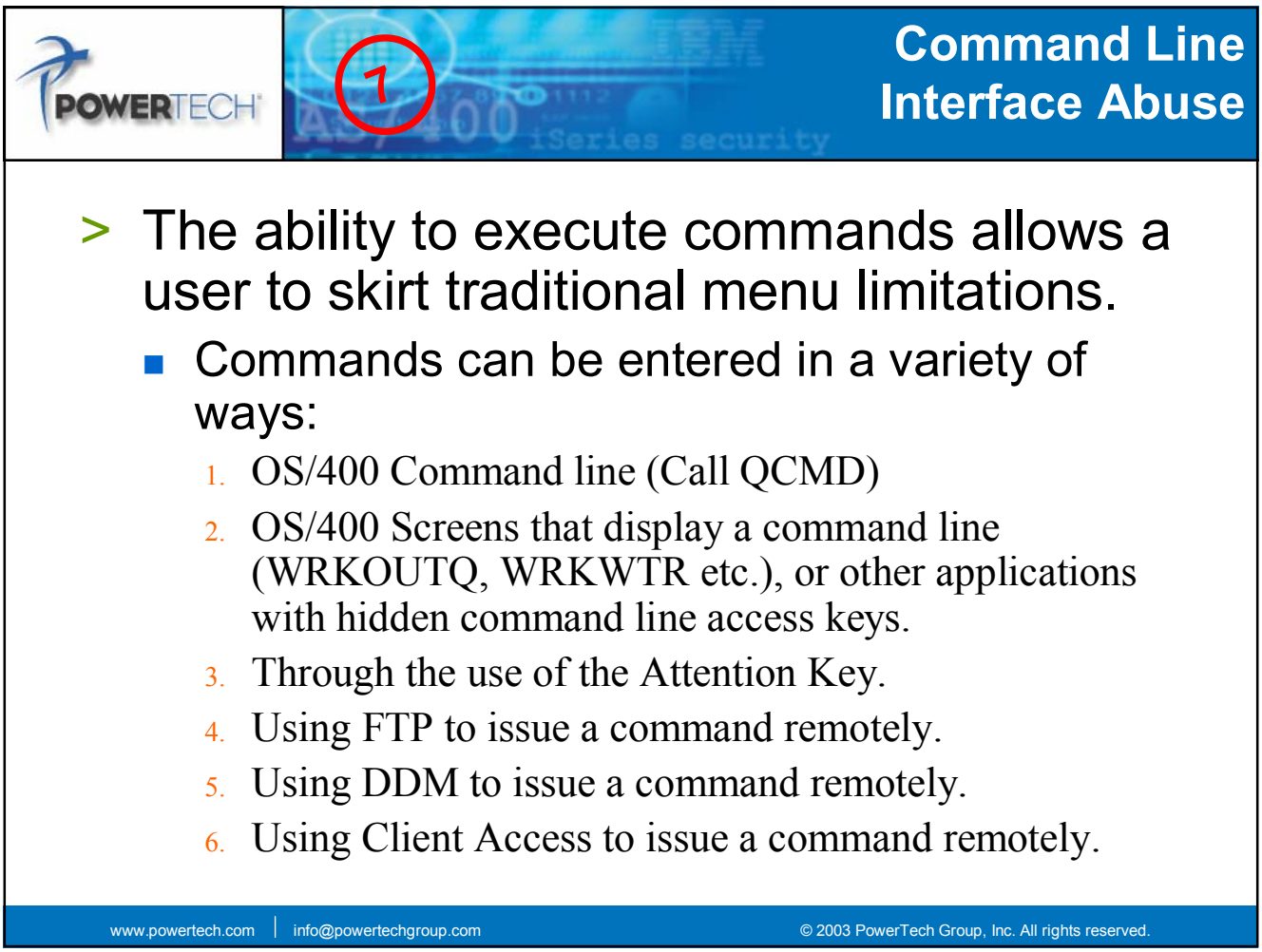
opyright (c) 1999 - 2002 The Powertech



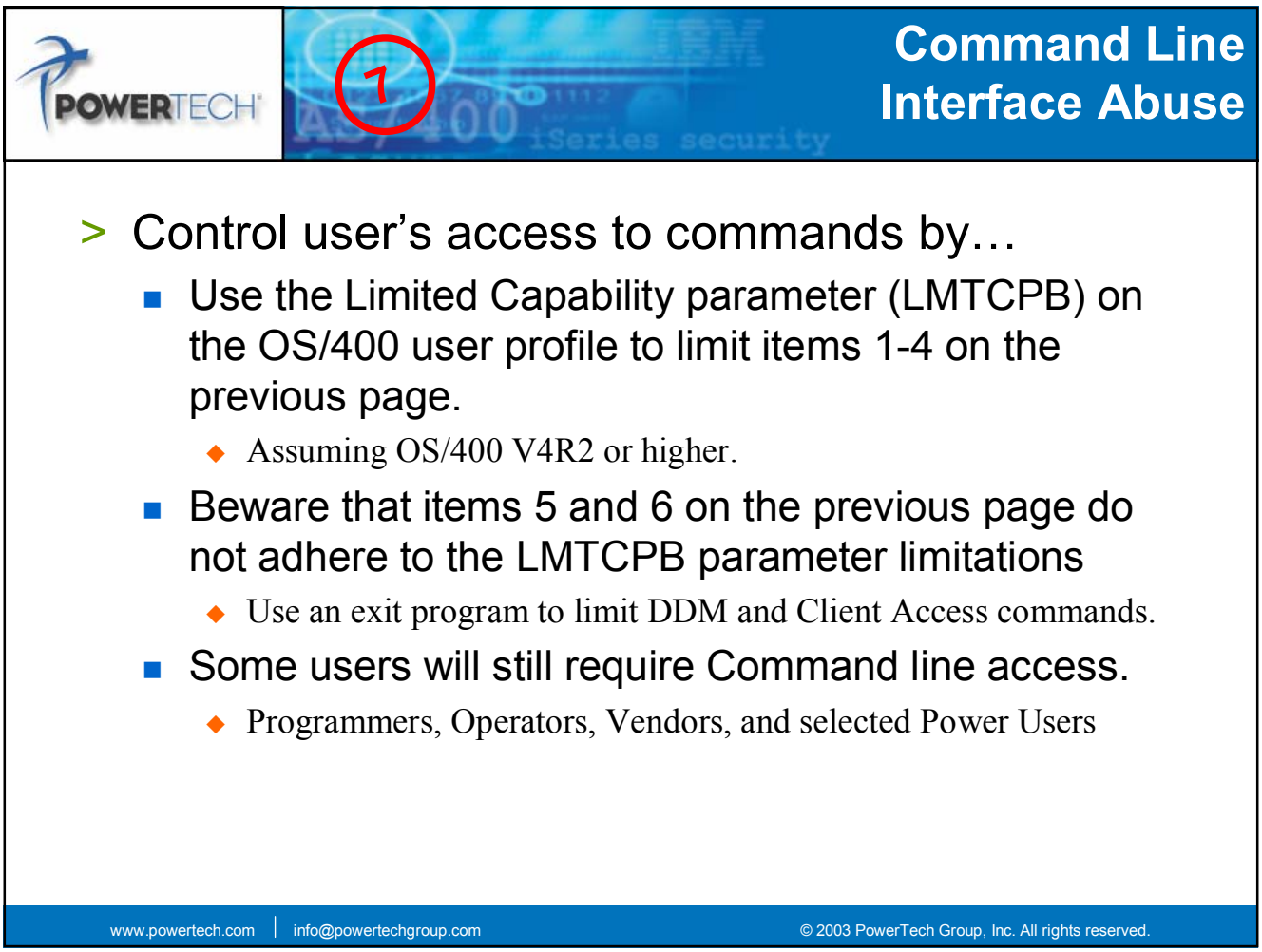
opyright (c) 1999 - 2002 The Powertech



opyright (c) 1999 - 2002 The Powertech

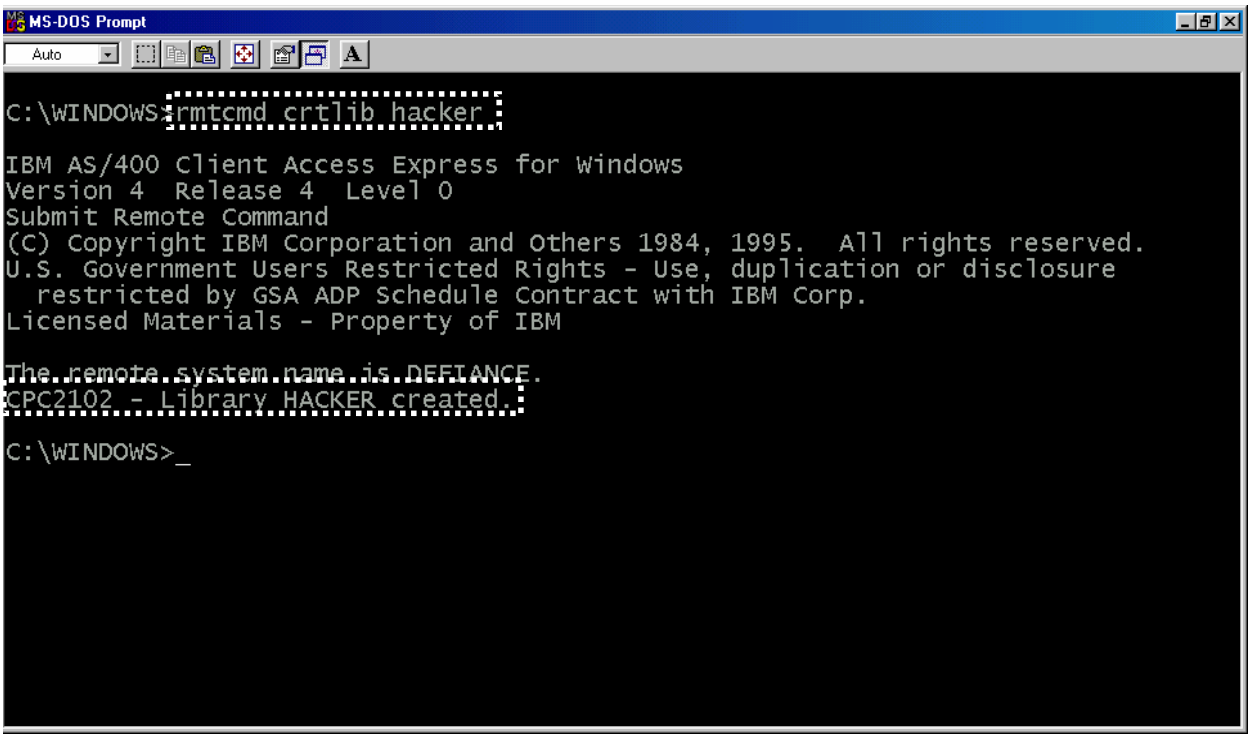


opyright (c) 1999 - 2002 The Powertech



opyright (c) 1999 - 2002 The Powertech

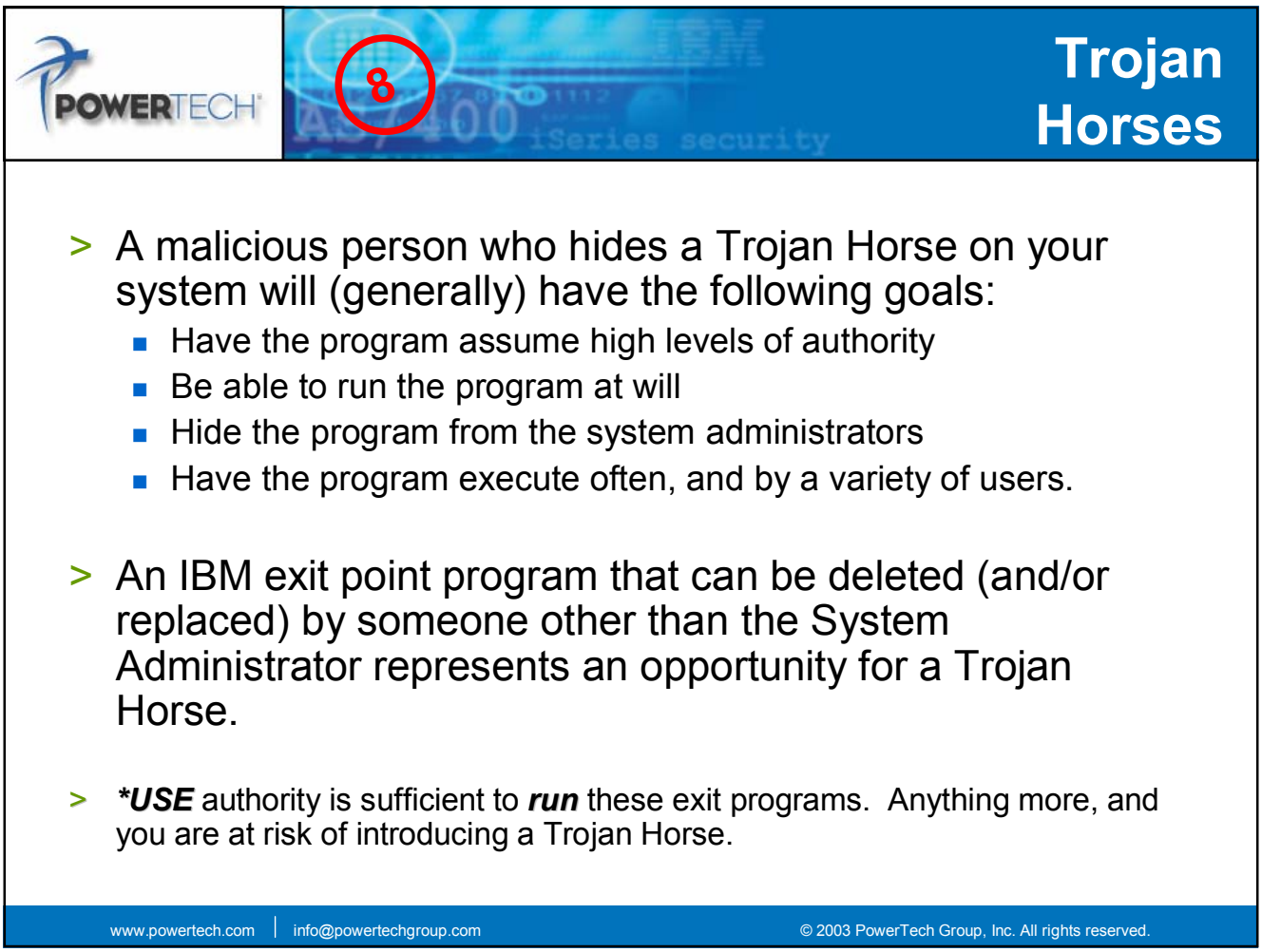
Command Line Interface Abuse



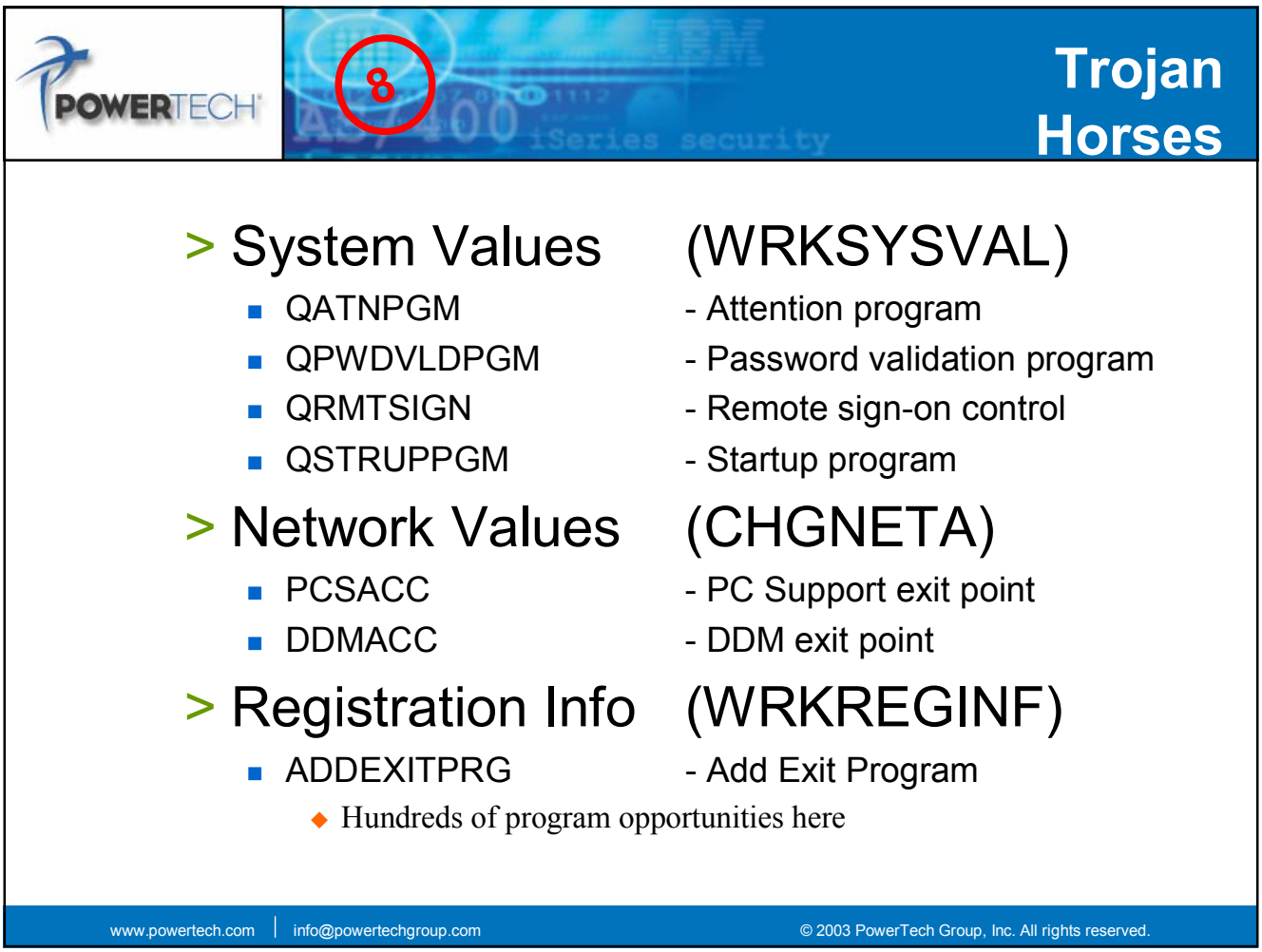
© 2003 PowerTech Group, Inc. All rights reserved.

opyright (c) 1999 - 2002 The Powertech

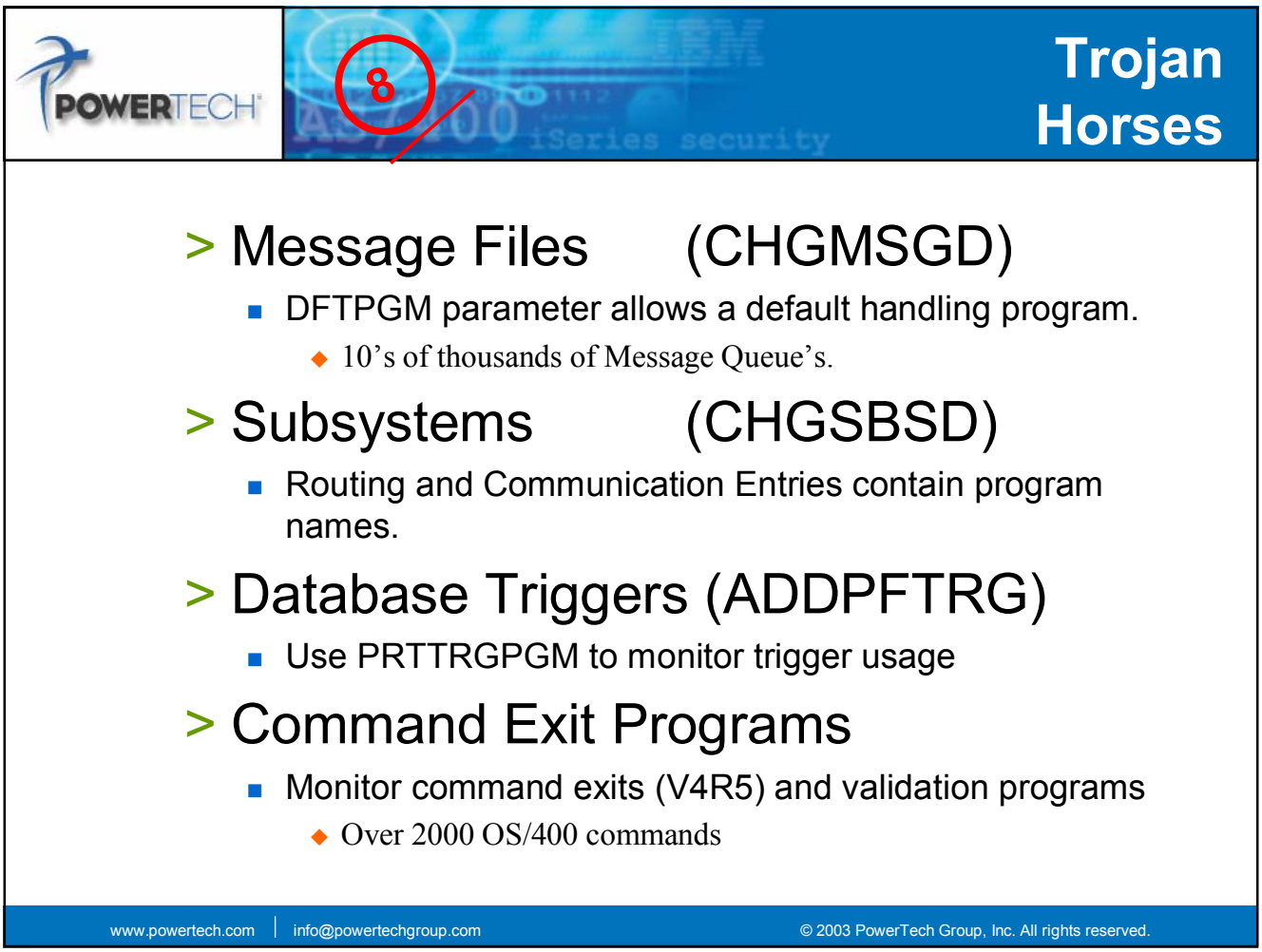
opyright (c) 1999 - 2002 The Powertech



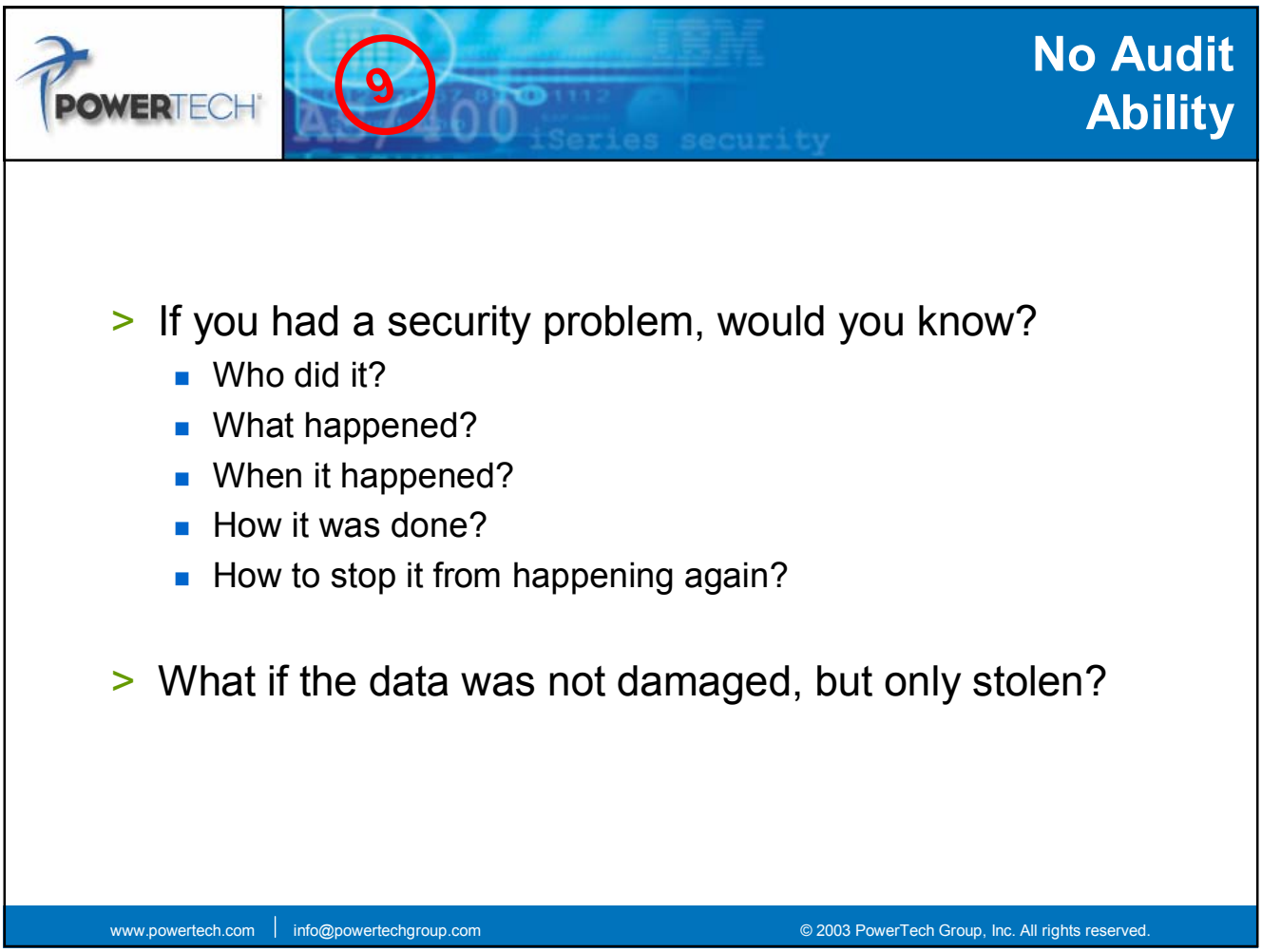
opyright (c) 1999 - 2002 The Powertech



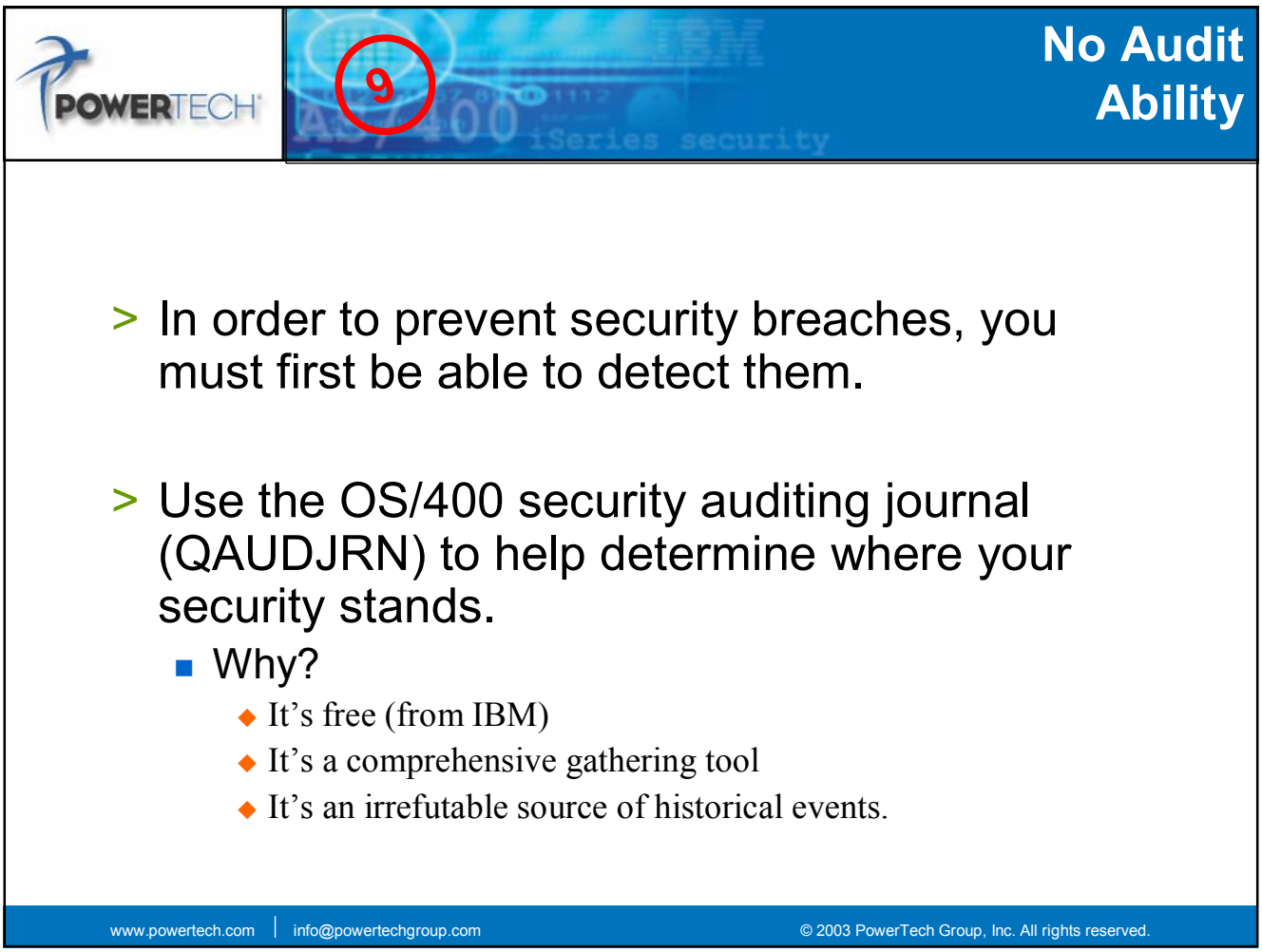
opyright (c) 1999 - 2002 The Powertech



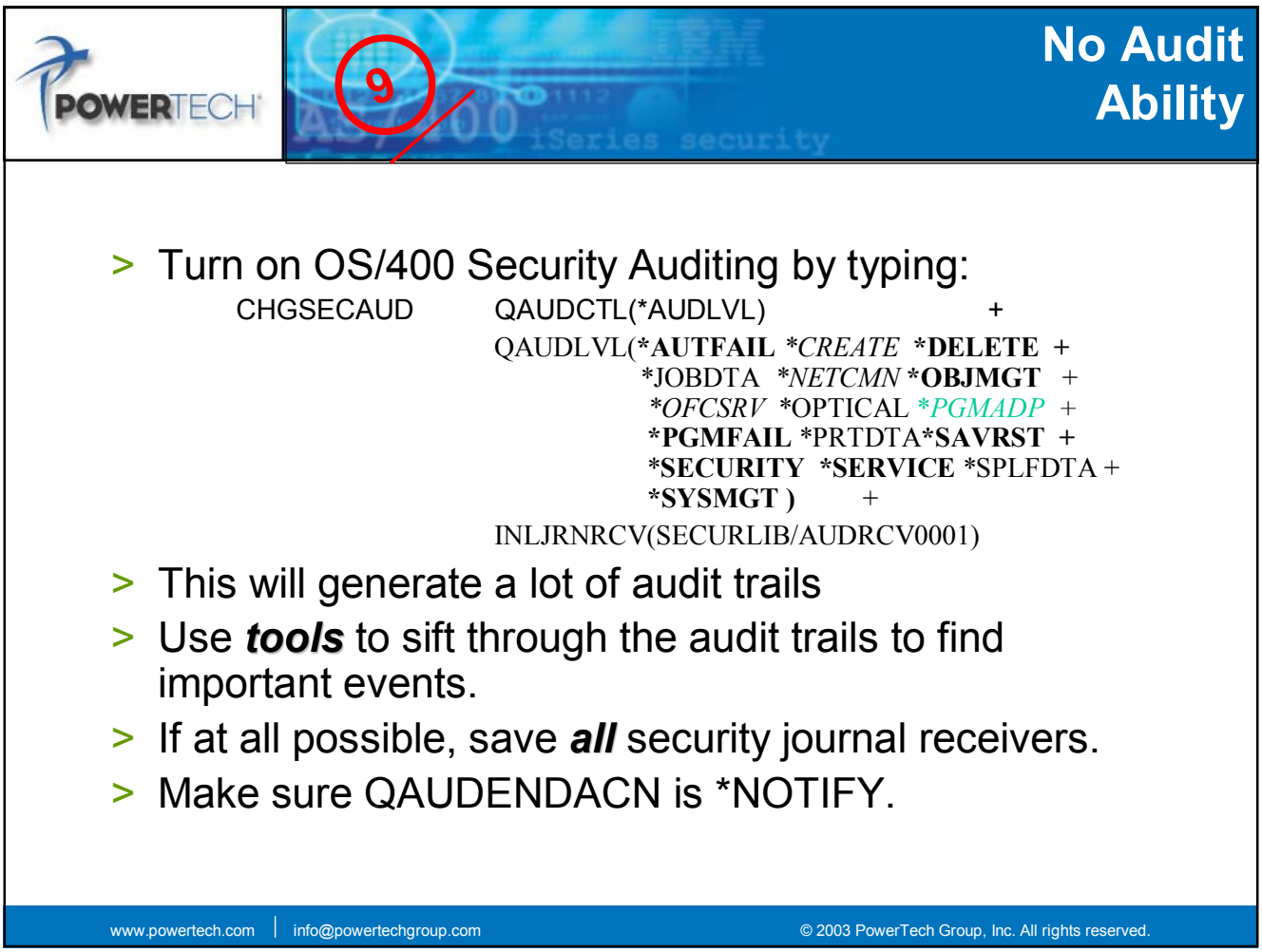
opyright (c) 1999 - 2002 The Powertech



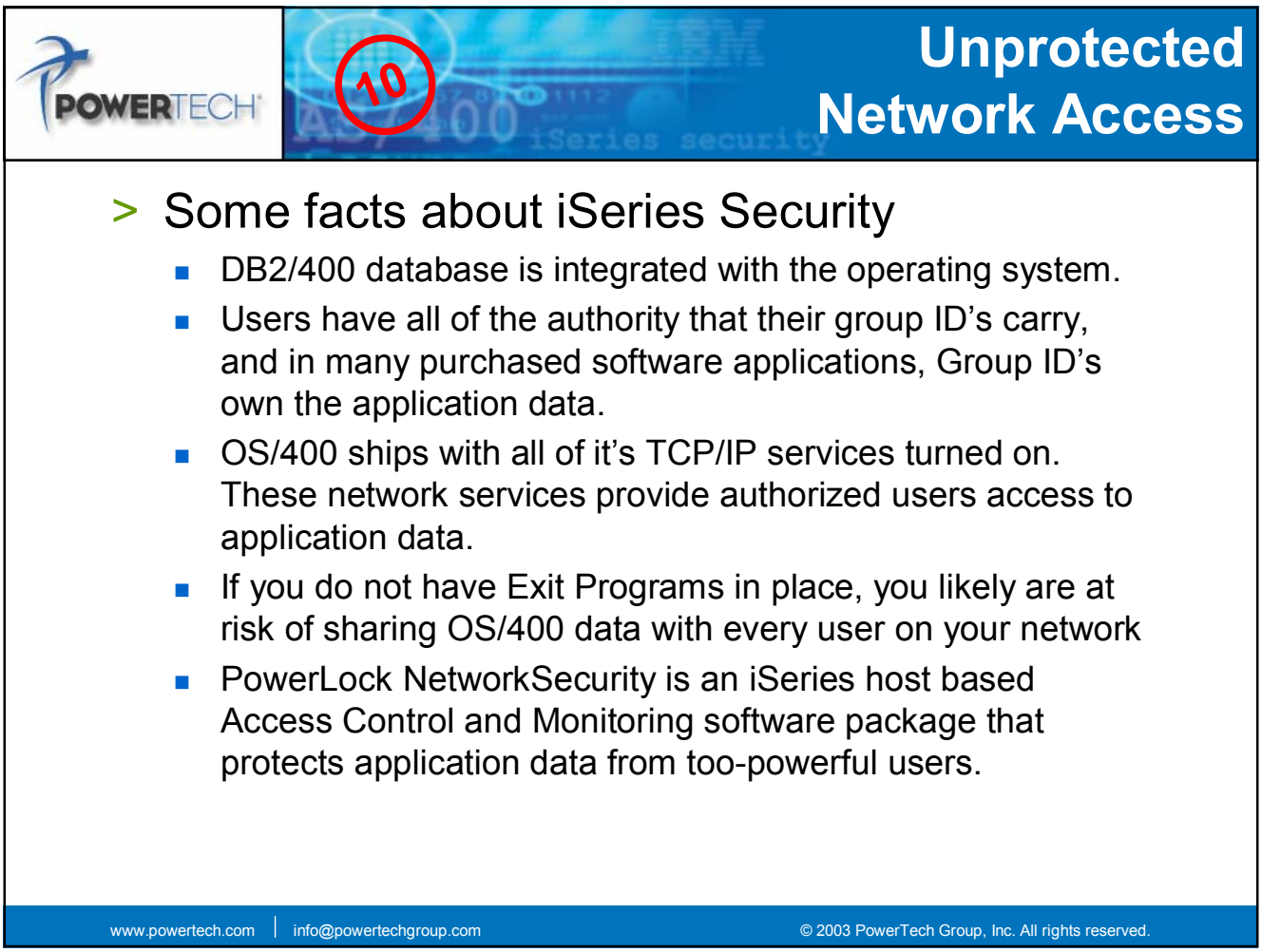
opyright (c) 1999 - 2002 The Powertech



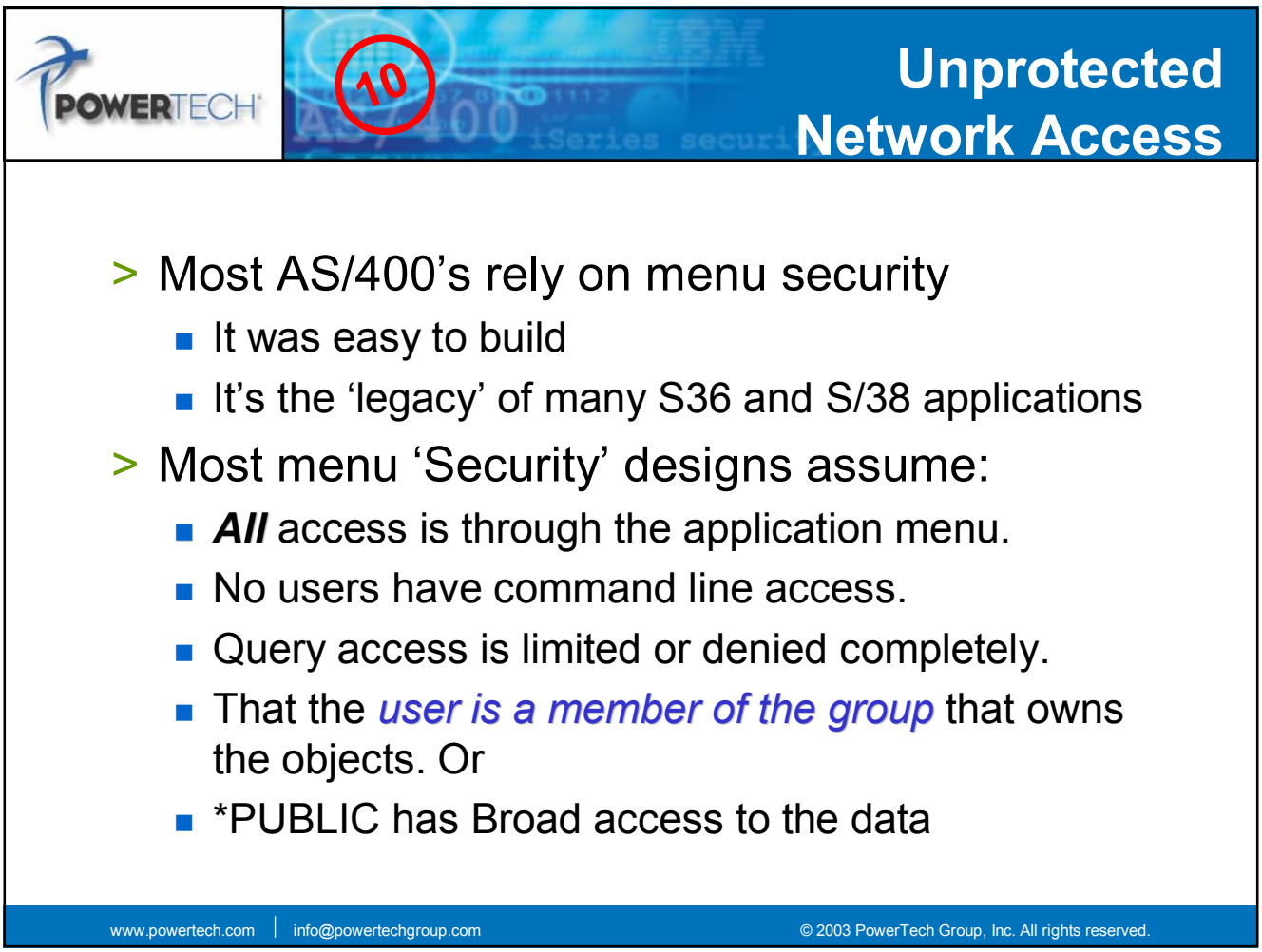
opyright (c) 1999 - 2002 The Powertech



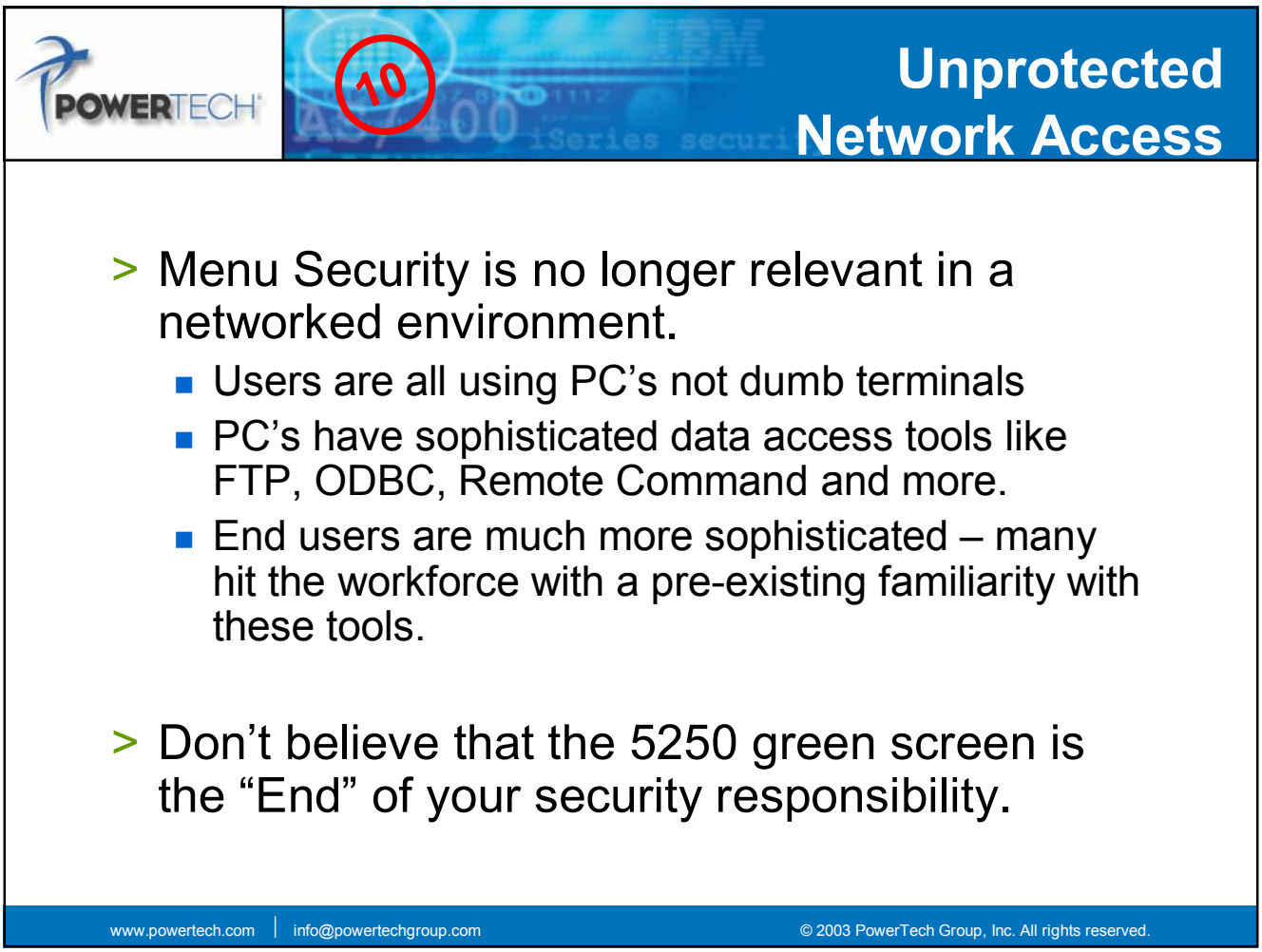
opyright (c) 1999 - 2002 The Powertech



opyright (c) 1999 - 2002 The Powertech

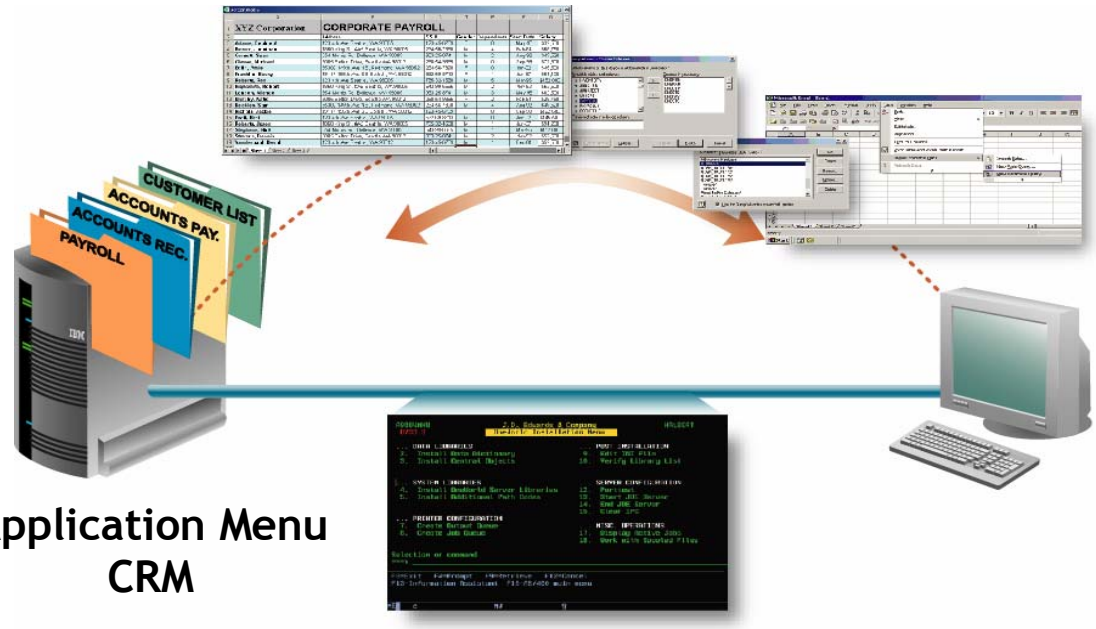


opyright (c) 1999 - 2002 The Powertech



opyright (c) 1999 - 2002 The Powertech

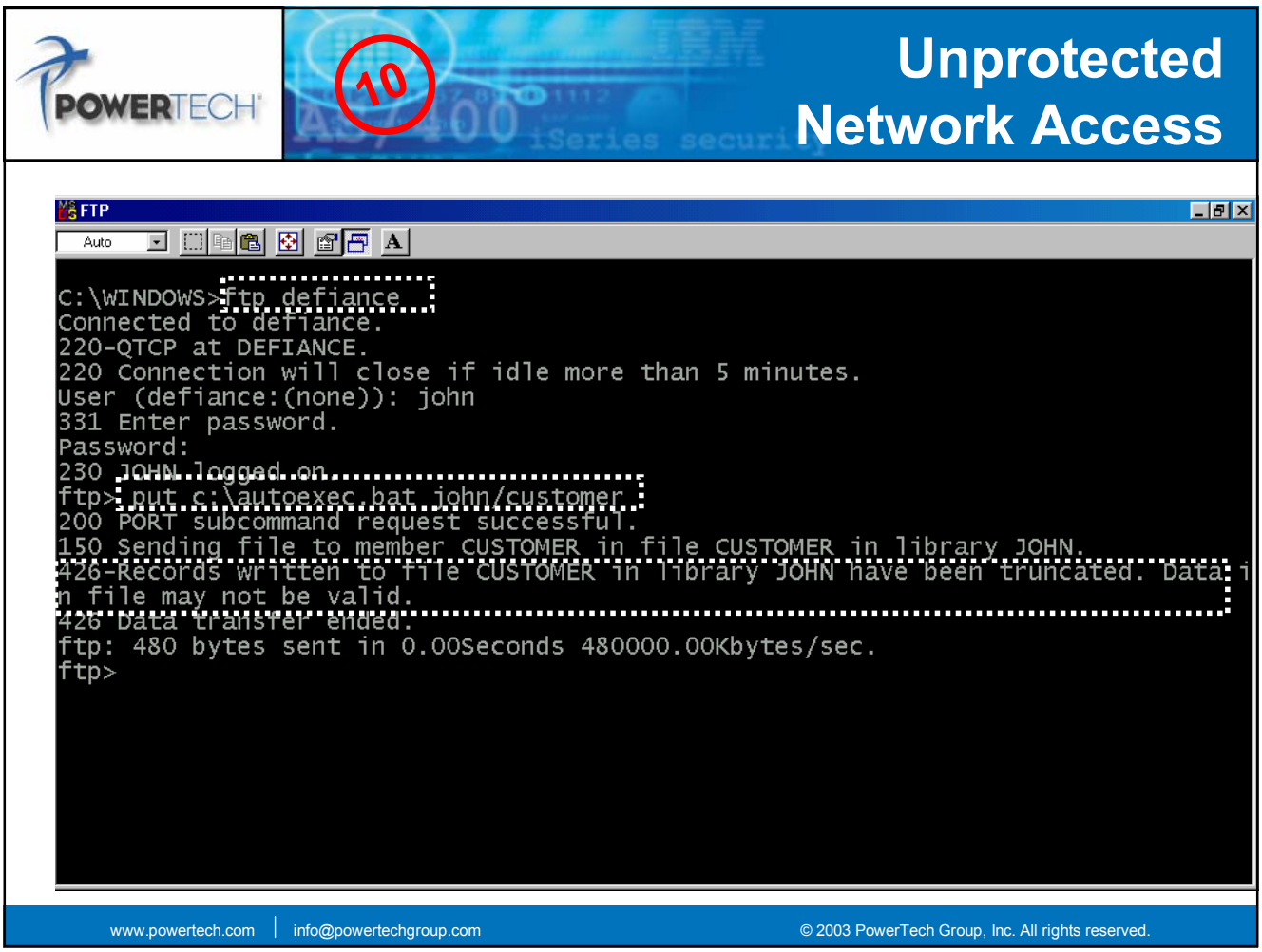
Result: Too Much Access



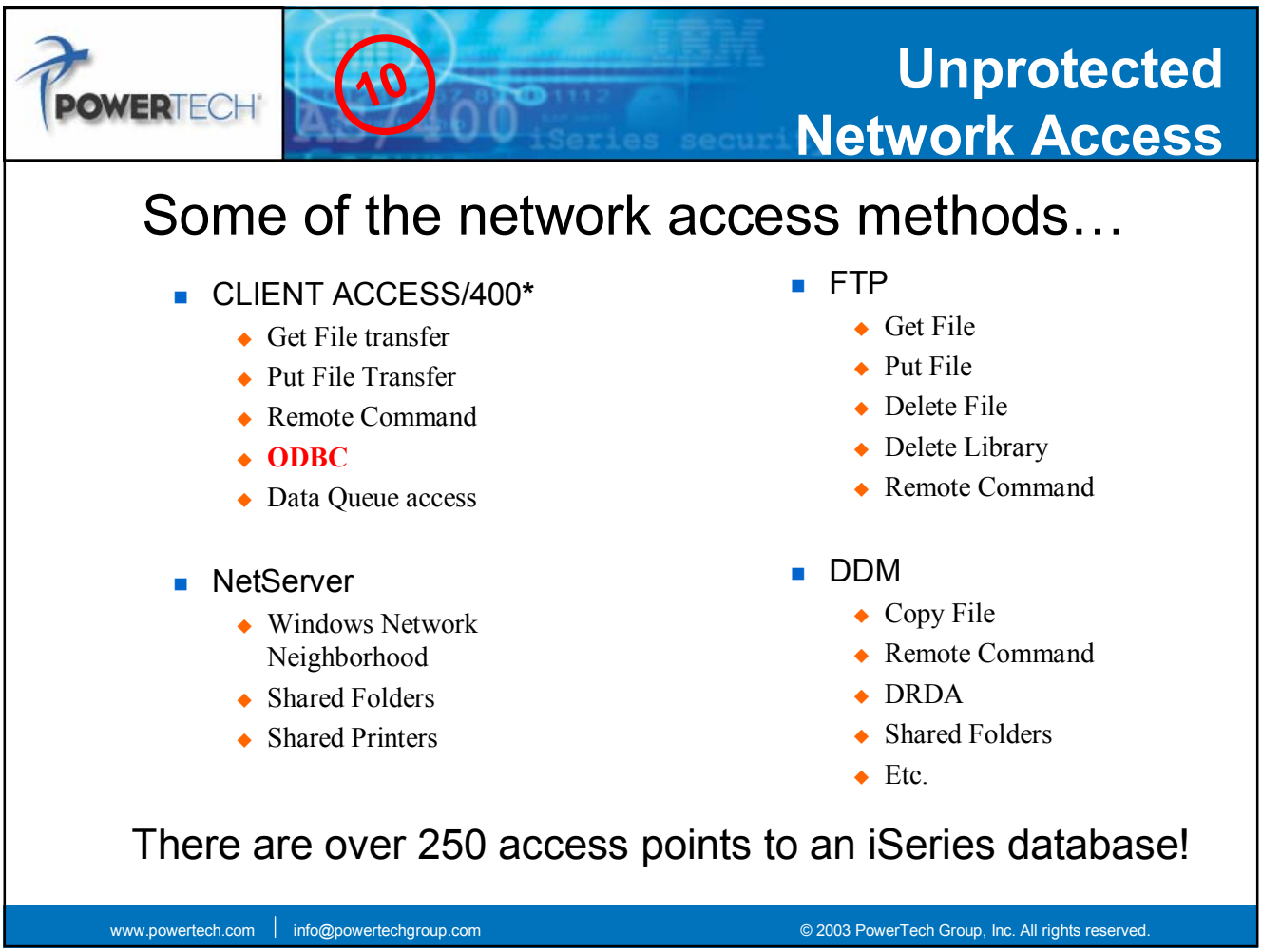
Application Menu
CRM

© 2003 PowerTech Group, Inc. All rights reserved.

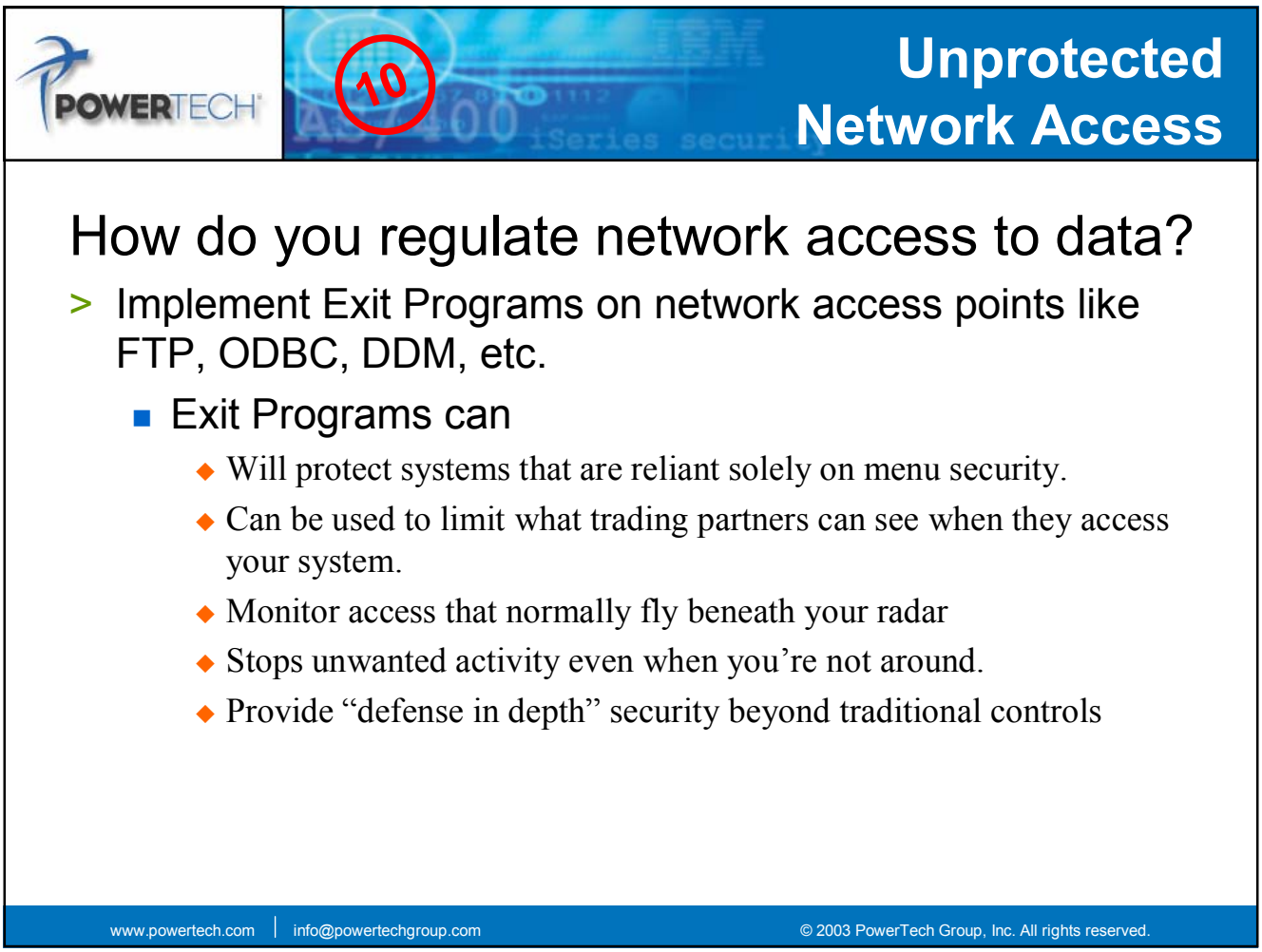
opyright (c) 1999 - 2002 The Powertech



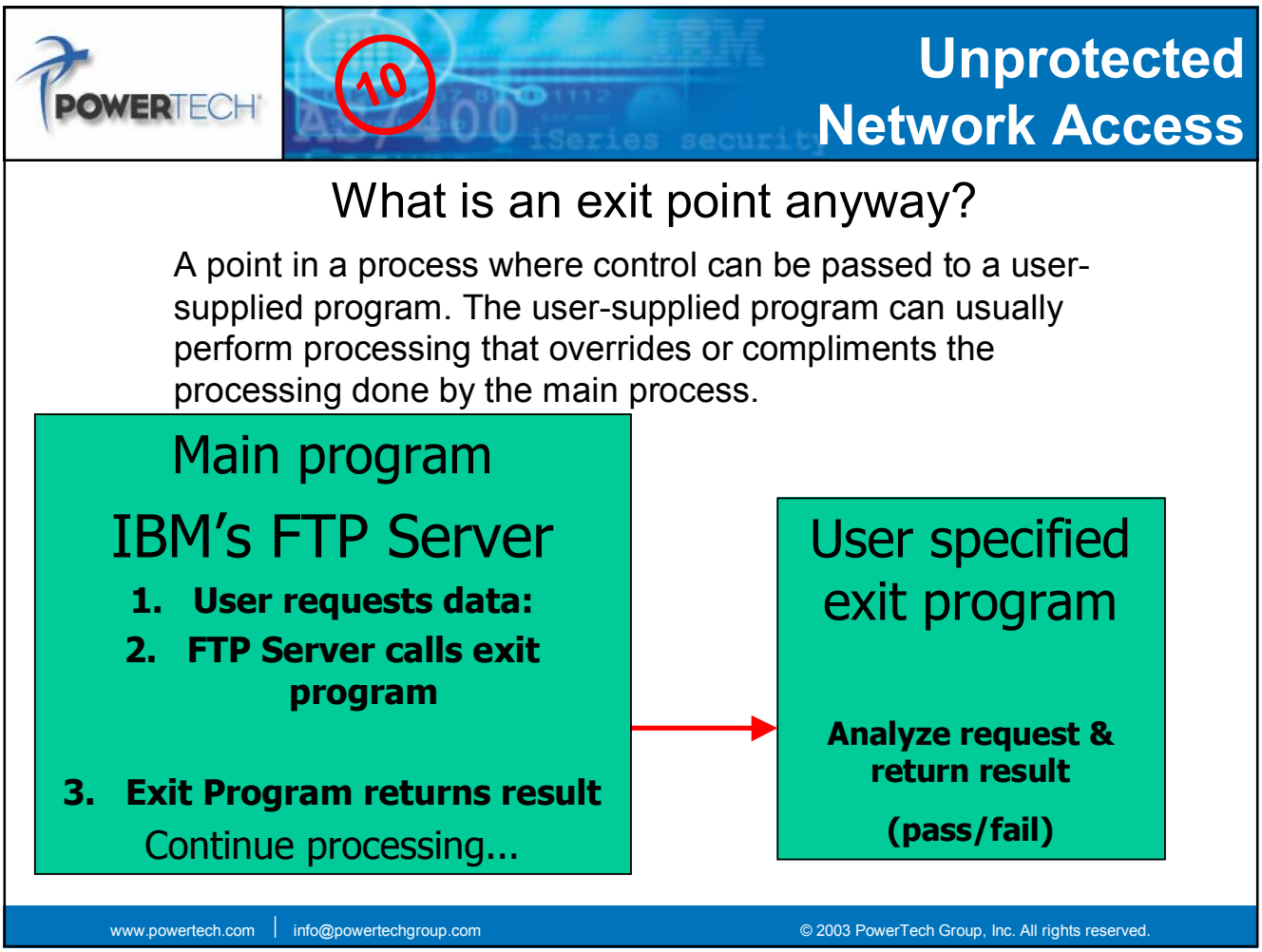
opyright (c) 1999 - 2002 The Powertech



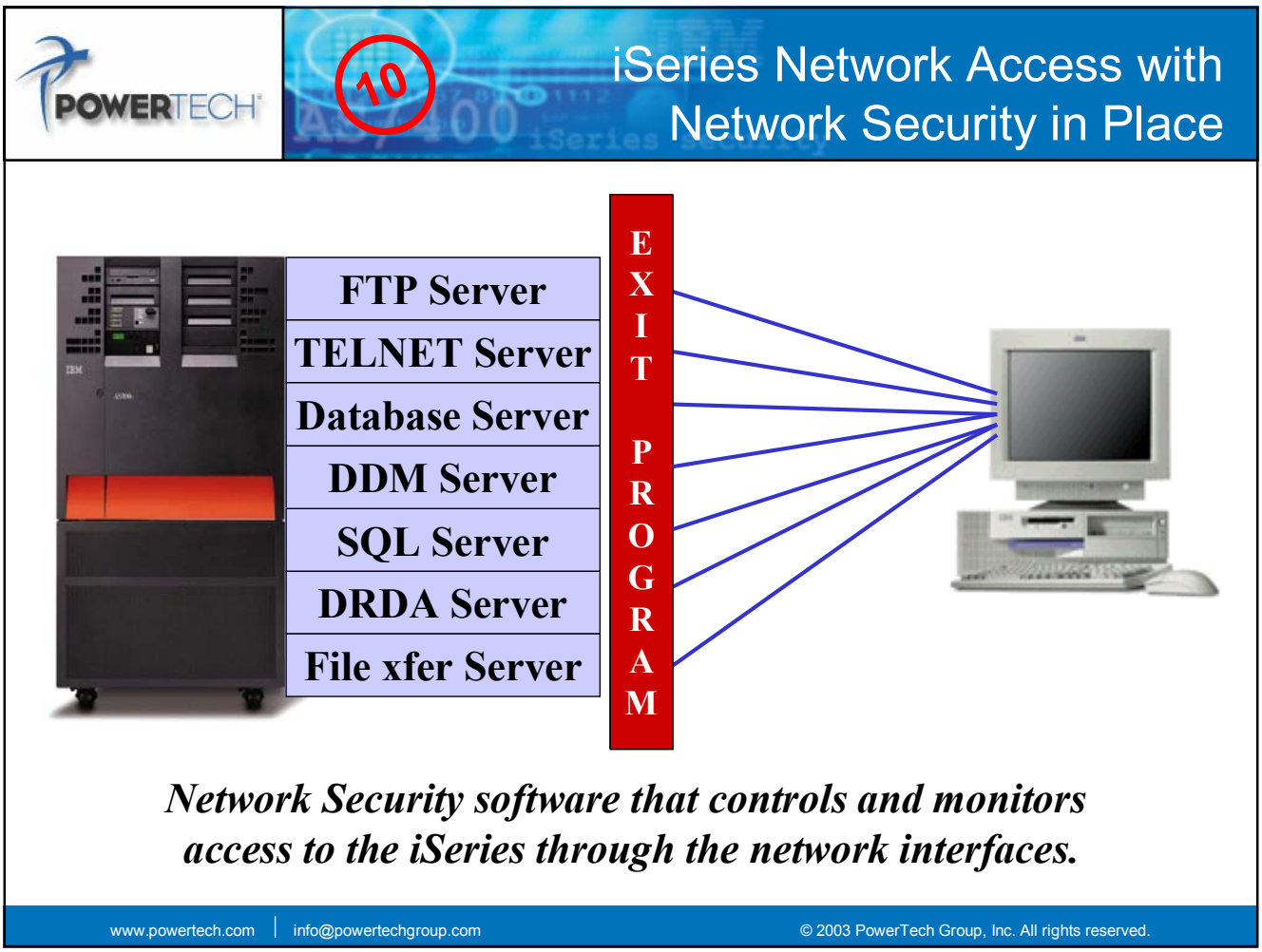
opyright (c) 1999 - 2002 The Powertech



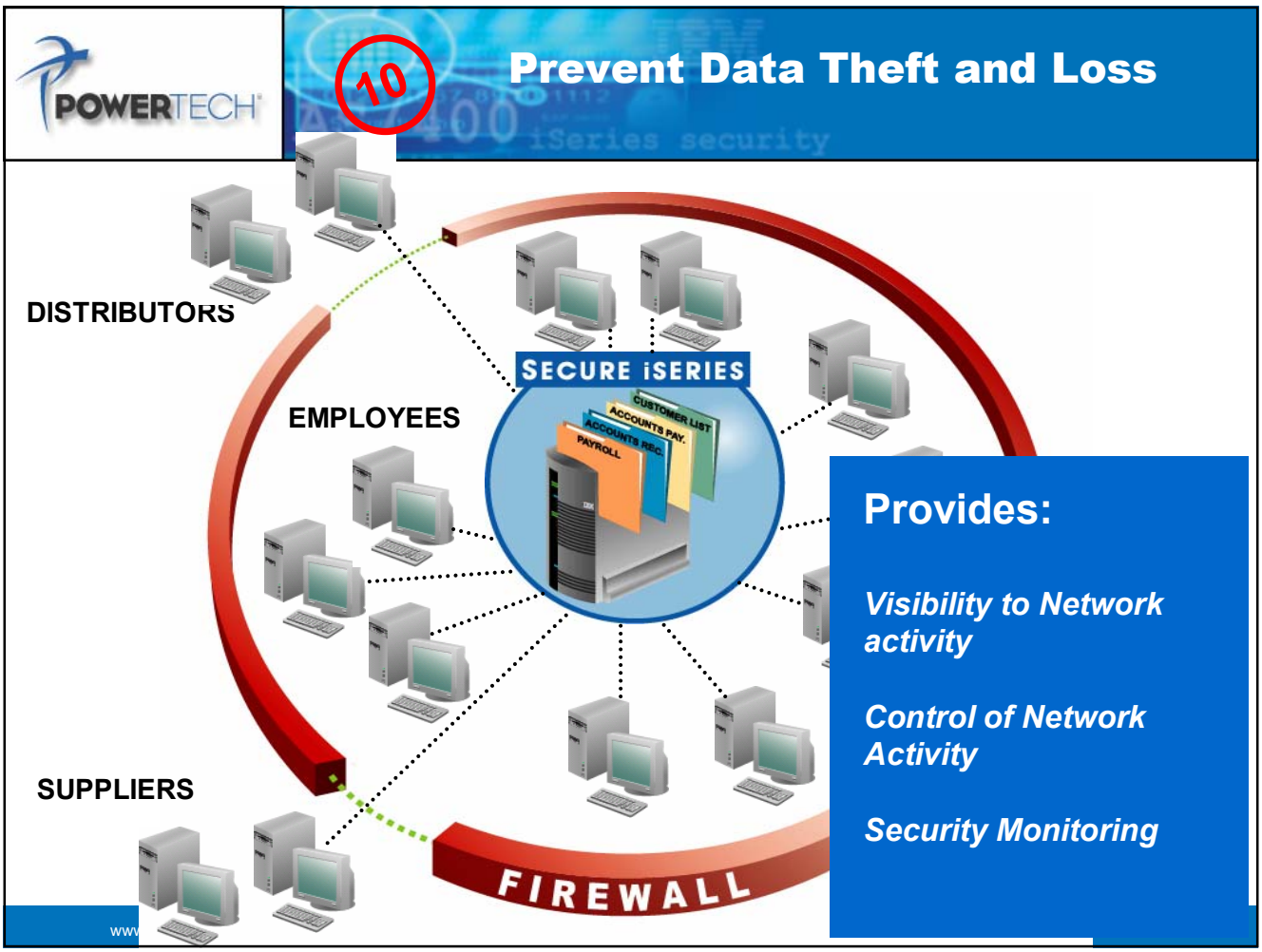
opyright (c) 1999 - 2002 The Powertech



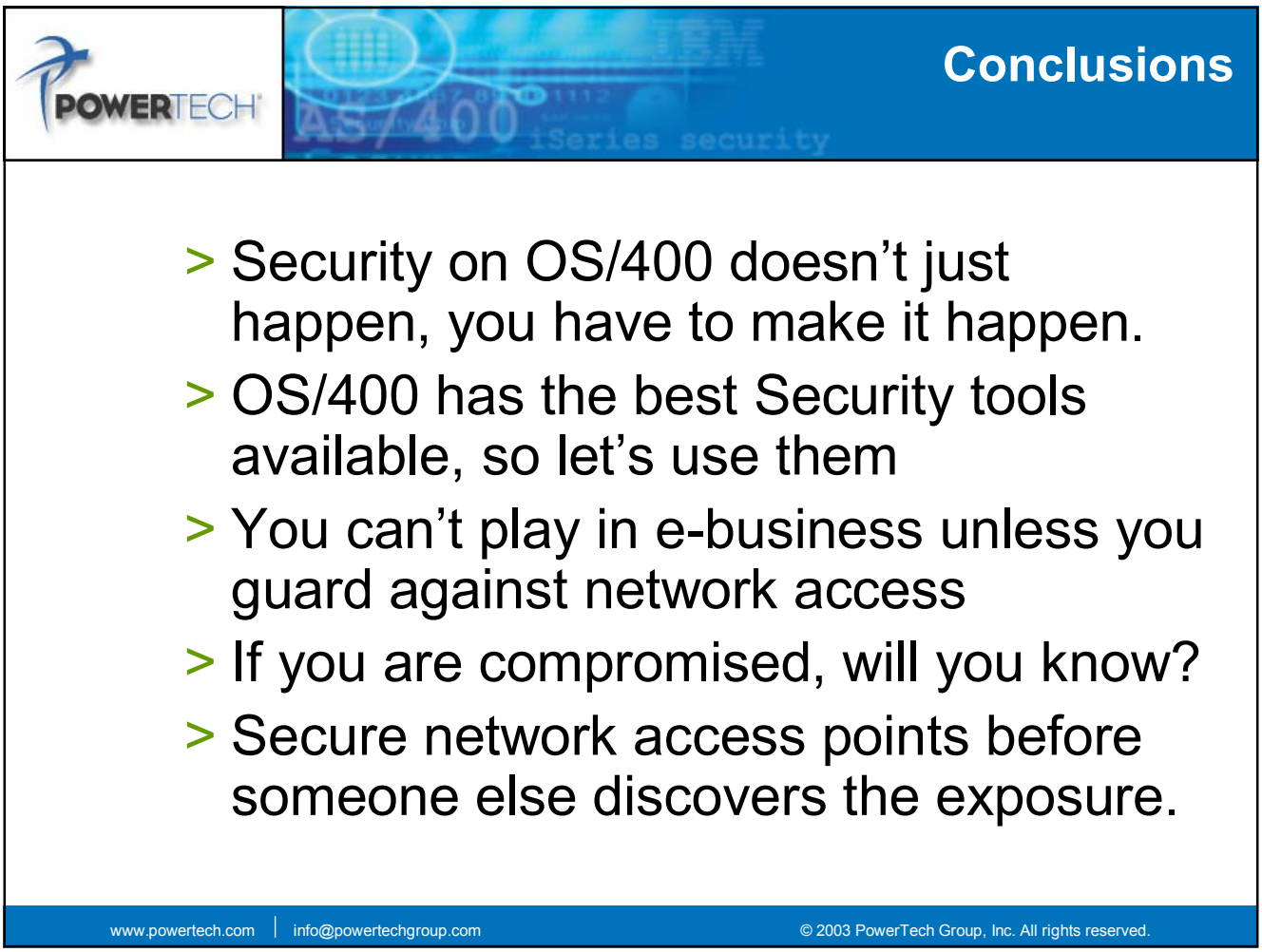
opyright (c) 1999 - 2002 The Powertech



opyright (c) 1999 - 2002 The Powertech



opyright (c) 1999 - 2002 The Powertech



opyright (c) 1999 - 2002 The Powertech

Thank You

Contact Info:

John Earl

Chief Technology Officer

The PowerTech Group

john.earl@powertech.com

253.872.7788 x302

© 2003 PowerTech Group, Inc. All rights reserved.

opyright (c) 1999 - 2002 The Powertech