Data Security

Protecting Your Personal & Professional Information

Kate Keeley
Small Business Community Rep.
719-359-7818
kate.keeley@qwest.com
www.qwestconnectthedots.com

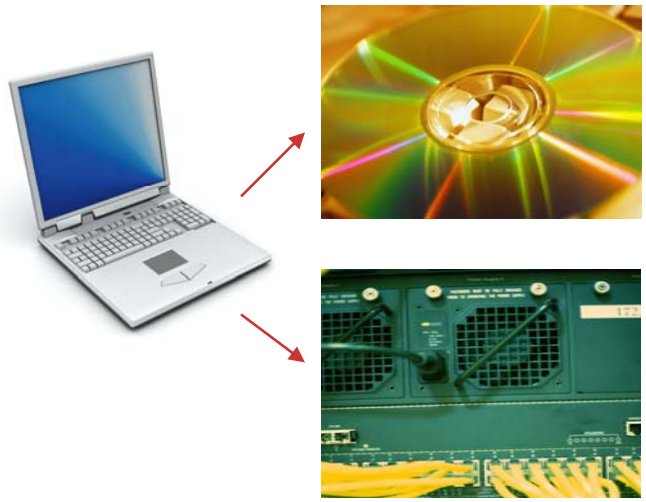
Sponsored by Qwest BUSINESS

Agenda

- What is data security?
- Why secure your data?
  - Risks when you don't
    - Intentional harm
    - Unintentional harm
  - Benefits when you do
- Security tips & techniques
- Q&A

What is data security?

Data Security means ensuring your critical business information is protected and can only be accessed by authorized users.



Intentional harm – Hackers, con-artists, or disgruntled employees attempt to gain unauthorized access, use, disclose, disrupt, modify, view, record or destroy information.

Unintentional harm – Data lost or compromised due to user error or hardware failure.

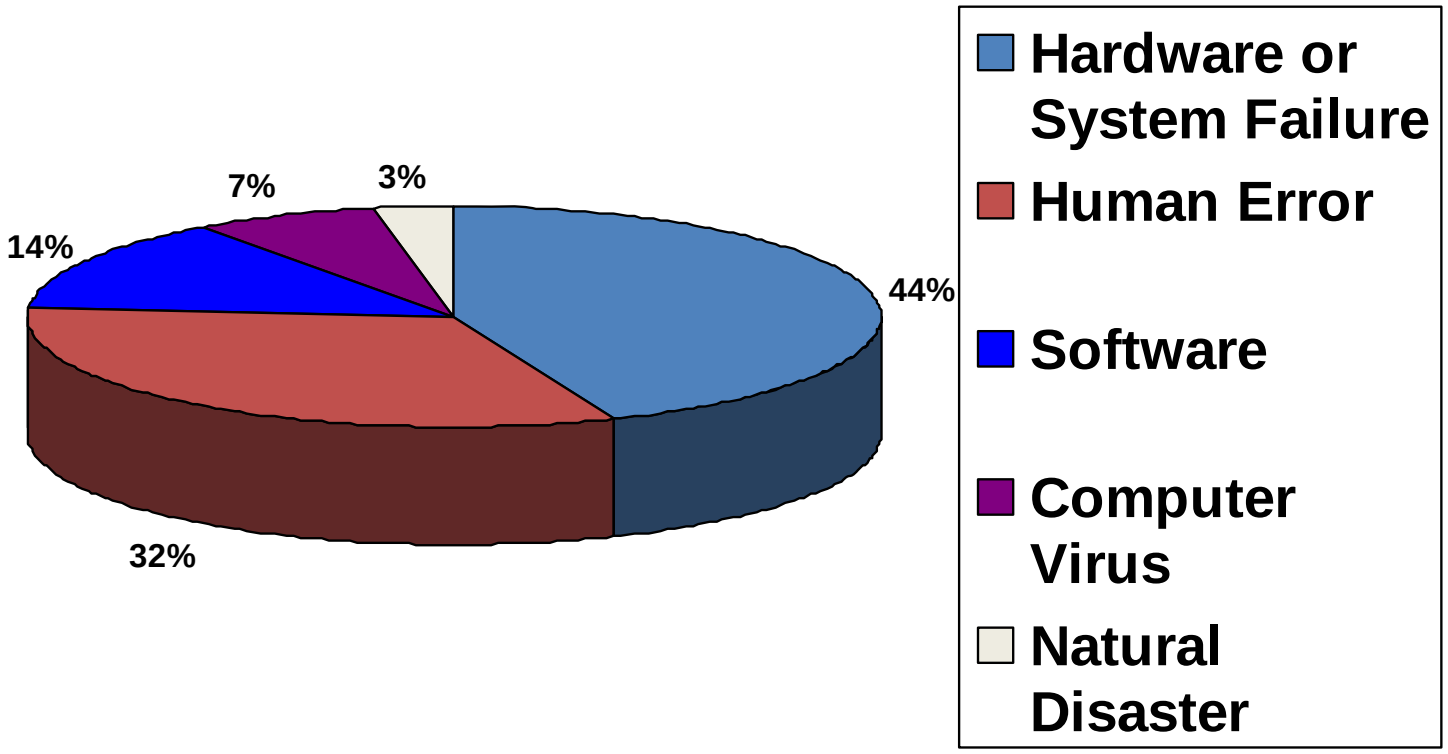
The cost to a company can total $197 per missing record when factoring in the loss of customers, legal fees and PR crisis management. --Ponemon Institute[1]

What are the risks?

- Critical information on your computer workstations, networks, portable drives, laptops and phones is vulnerable to:
  - Accidental loss
  - Hard drive failure
  - Theft
  - Data corruption
  - Employee sabotage
  - External attacks
  - Natural disasters
  - Power outages
- You may be legally required to back up your data

What's the most common cause of data loss or compromise?

Causes of data loss by frequency[1]



7 of 10 small firms that experience a major data loss go out of business within a year

Who needs data security?

- Does your company…
  - request payment information or health data electronically?
  - request personal data like social security numbers, credit card numbers, or any other personally identifiable information electronically?
  - encrypt important information leaving the network?
  - permit employees to exchange electronic documents as part of their daily work routine?
- Do you…
  - provide payment information or health data electronically?
  - provide personal data like social security numbers, credit card numbers, or any other personally identifiable information electronically?
  - encrypt important information leaving your home network?
  - exchange electronic documents with friends and family?

What is the most common cause of identity theft? How many incidents of identity theft are attributable to online breaches?[1]

Data source: Studies cited in 9 January 2011 article by PRWeb[1]

Identity theft

- 80% of Americans are concerned
- 12% of Americans are enrolled in an identity theft protection program
- Number of US victims nationwide: 11.1 million
- Cost of identity theft if violated: $4841
- Average out-of-pocket expense to victim: $527
- Total cost of identity theft to businesses: $54 billion
- Cost of protection services: $250

What's the weakest link in most security plans?

The weakest security link[1]

- Passwords, the weakest link
  - In 2009, an 18-year old hacked a Twitter administrator's account and accessed several high profile accounts, including President Barack Obama's.
  - The password that gained this hacker access: "happiness."[2]

What's the worst password?

Create a strong password

- Creating a strong password
  - Don’t use dictionary words
  - Don’t use words common to your life (SSN, phone, address, birthdays of close family)
  - Use a combination of capital and small letters, symbols, and numbers
  - Consider creating a phrase that’s easy for you to remember and then using just the first letter of each word
    - My best friend’s name is Nancy Wood; her area code is 321. Password: MbfniNW;haci321
    - Best idea: Use unique passwords for all (or at least all important accounts)
    - Next best idea: Create passwords that you can use in more than one place by applying the above guidelines and using just the first or second half of the compound sentence if the whole phrase is too long.
  - Change passwords on a regular basis
  - Be sure that a process exists to remove anyone who leaves the organization from password protected sites and change the passwords

How long does the average employee spend each day using the Internet for personal reasons?

Networks: Prevention is the best protection

The average employee spends between one and two hours each day using the Internet for personal reasons. --Wise Geek[1]

- The best way to protect against inappropriate usage and data compromises online is to set up clear policies and communicate them to employees
  - File sharing
  - Webmail
  - Web usage
- Firewalls
- Virus/spyware protection software
- Computer/Internet usage-monitoring software
  - Time Doctor
  - Work Examiner
- Web filtering
  - Blacklisting (restricting access to inappropriate sites)
  - White-listing (giving access to appropriate sites)
- Buyer Beware: Purchasing online
  - Only buy from companies you know and trust
  - Resist offers that push you to “act now” to save more
  - Read the small print
  - Get offers in writing
- Disconnect from the Internet when not in use

Email and instant messaging

- Create an authorized use policy
  - Business use only?
  - Communicating with family
- Be aware of the content passed back and forth
  - No personal data like SSN, credit cards, insurance information
- Ensure that the application has the appropriate malware protection
- Don’t open or automatically click on links/URLs in emails
  - Over 90% spam sent in 2009 contained a URL and many led to one of over 30 thousand websites hosting malicious software[1]
  - Example: Rumor that Facebook was going to start charging a monthly fee and encouraging people to navigate to a “protest” page that, in reality, hosted malicious software[2]
  - Be especially careful with anyone asking for financial information
- Report spam[3]
  - Forward spam to the FTC at spam@uce.gov and to the abuse desk of the sender's ISP.
  - Also, if the email appears to be impersonating a bank or other company or organization, forward the message to the actual organization.

Can you name one of the top 10 email scams?

Top 10 scams to filter out of your email[1]

- The "Nigerian" Email Scam
- Phishing
- Work-at-Home Scams
- Weight Loss Claims
- Foreign Lotteries
- Cure-All Products
- Check Overpayment Scams
- Pay-in-Advance Credit Offers
- Debt Relief
- Investment Schemes

What was rated the most common malware in 2010 by McAfee?

Stats: Malicious software (malware)

- Approximately 55,000 pieces of new malware appear every day[1]
- The most common malware in Q2 2010 targeted portable storage devices [2] and took advantage of the “auto run” feature in Windows
- PDF hack allows malicious downloads of executable files without exploiting any inherent weakness in the user’s system[4]
- Dictionary attacks (or why you shouldn’t use easy passwords)
  - Password cracker
- MAC user alert[3]

What is one of the best ways to protect your wireless network?

Wireless security

- Change default admin passwords on routers immediately
- Keep your hardware updated and upgraded because hackers are always looking for (and finding) ways to crack security
- Turn on WPA2 security
- Change the default SSID
- Don’t set your computer to auto-connect to wireless networks
- Enable firewalls on the router and all computers that connect to the wireless network
- Monitor your network traffic with tools like Network Magic Pro (~$40), Who’s on my WiFi, or AirSnare
- **Turn off the network when not in use for extended periods of time**

According to Mobiledia, which smartphone OS saw the greatest increase in malware attacks in 2010?[1]

Smartphones

Malware attacks against smartphones rose by one-third in 2010 --Mobiledia[3]

- Mobile phones are on the verge of overtaking PCs as the most common method of accessing the Internet[1]
- More vulnerable to almost every imaginable data threat
  - Loss or theft
  - Hacking
  - False-front websites posing as authentic sites
  - Malware downloads
- Smartphone apps may be transmitting users' personal information, including unique phone ID numbers, without their permission, revealing the extent to which online ad networks will gather personal data about consumers[2]

How many people in this room are likely to have a laptop stolen?

Protect against intentional harm: Theft

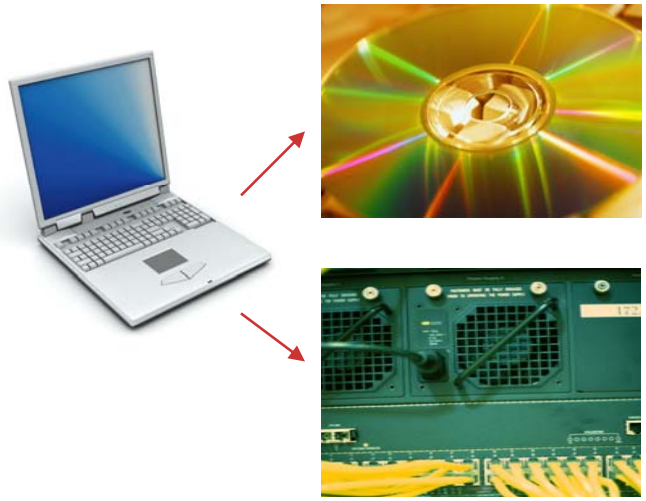
- Theft
  - One out of 10 laptops are stolen within 12 months of purchase[1]
  - 97% of stolen laptops are never recovered
    - Are the passwords on your laptop auto-saved?
    - Are electronic copies of bank statements saved on the hard drive?
- Prevention
  - Encryption is the best protection against information breach
  - Lock up laptops or don't leave them unattended

Security policies

- Create them
- Document them
- Validate them
- Approve them
- Communicate them (include reminders)
- Use them
  - Ensure they are flexible enough to change with company needs
- Enforce them
  - Create additional policies for those in administrative and supervisory roles that address the scope of their responsibilities

Recovering lost or damaged data

Data Protection ensures the security and availability of your critical business information against unintentional harm by using offline or online data back up.



Offline Data Backup – You can save your files to physical media such as digital tapes, virtual tape libraries, CDs, DVDs, external hard drives, on-site servers, virtual servers, and network attached storage.

Online Data Backup- You transmit your data to a remote location and store it on servers.

Why should you care?

Small Business data loss incidents are followed by lost sales in 30% of cases, lost customers in 20%, and severe business disruption in 25% of cases.

"SMB Protection Gap." Symantec, 2009. www.symantec.com/business/solutions/article.jsp?aid=20090428_global_study_identifies_smb_security_gap

Backup – pros and cons

Offline	
Pros	**Cons**
Affordable Cost	Storage risks due to onsite location and increased costs if backup offsite
Fast Recovery	Physical vulnerabilities due to wear
Practical for mobile team without network connection	Need to manage back up schedule

Online	
Pros	**Cons**
Lead IT burden	Restoration speed can be slower
Flexibility for growth	Security
Mobile access	Upload speed
Option of continuous data protection (CDP)	Provider continuity

Implementing data protection: Next steps

Data Backup is not complicated to get started

1. Identify the information you need to back up
   Mapping out your vital information will help you determine how and when to back it up.

2. Choose your backup solution
   Compare backup technology options.

3. Set a backup schedule
   How frequently you back up your data will depend on what kind it is and how often it changes.

4. Test and review your solutions regularly
   Test whether your new backup system can do a full recovery of all your data shortly after launch, then do a test restore once every few months. (If you use a hosted solution, ask your vendor how often they test the system.)

Most important idea

Protecting your data
helps you recover faster,
saves time & hassle,
prevents lost sales,
and is easy to implement.

Resources

- The organizations listed below provide valuable information on specific standards or examples of security governance standards:
  - International Organization for Standardization (ISO)
  - The USA National Institute of Standards and Technology (NIST)
  - The Internet Society
  - The Information Security Forum
- To report spam
  - Forward spam to the FTC at spam@uce.gov and to the abuse desk of the sender's ISP.
  - If the email appears to be impersonating a bank or other company or organization, forward the message to the actual organization.
- McAfee's Threats Report

Disk drive comparison

	SATA	SAS	SSD
Cost	★		
Capacity	★		
Reliability		★	
Expandability		★	
Simplicity	★		
Speed (e.g., data transfer rates)		★	
Green			★

SSDs are generally considered superior to hard disk drives.

It is possible to have a SAS SSD.

Overwriting data is not as efficient, historically cost tended to be the main prohibitive factor.

Top 10 scams to filter out of your email[1]

- The "Nigerian" Email Scam
- Phishing
- Work-at-Home Scams
- Weight Loss Claims
- Foreign Lotteries
- Cure-All Products
- Check Overpayment Scams
- Pay-in-Advance Credit Offers
- Debt Relief
- Investment Schemes

Thank you

See me after the presentation to talk about how online marketing, or other technology solutions, may be able to help your business.

Kate Keeley
(office) 719-636-4576
(wireless) 719-359-7818
kate.keeley@qwest.com

- Visit my blog at Qwest.com/connectthedots/colorado-springs

Benefits of data protection

- **Recover from incidents faster and more reliably**

  This allows you to recover quickly and stay open in the face of a computer crash, computer virus, or even physical loss

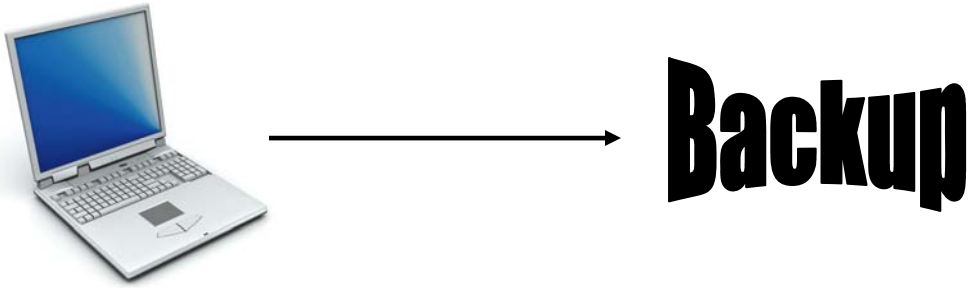
- **Save time and hassle**

  If you standardize the data back up process, efficiency improves and your management burden decreases. There are also ways to automate backup with certain backup tools.

- **Enjoy greater control and stability**

  When you have the right solutions and support to reduce data risks, you keep the focus on building your business, not rescuing it.

Can protecting your data save your business?



- Dean Parnell was often the only IT resource in a number of small businesses throughout his 13-year career.
- Parnell identified four areas where Small Businesses are lacking or fail
  - Make data backup an ongoing priority
  - Update backup solutions as data outgrows them
  - Develop an emergency plan for data loss incidents and educate employees
  - Test their data backup and recovery systems (quarterly or annually)
- “Most small businesses don’t realize what data backup does for them until they have a problem and it’s not there,” Dean points out. “That’s what happened in a DVD replication business I worked for.”