Examples of Cybersecurity Risks

Threat	Risk	Prevention/Mitigation
Physical theft	• Steal your smartphone, laptop, etc. • Acquire data from device	• Physically secure device • Password on device • Minimize data accessible from device • Encrypt data • "Find My Device" • Remote wipe
SQL injection	• Common attack against databases (such as credit card database) • Improperly-configured databases allow commands to pass through to it • Your data may be in this database	• Little consumers can do to prevent attacks • Minimize amount of data you share • Use unique passwords and security questions for each service
Cracking	• Attacker tries many username/password combinations – "Brute Force" attack • Once password is "guessed," attacker has full access • If attacker gains access to email, can then reset passwords for other accounts	• Do not use common passwords • Unique passwords per account • Two-factor authentication • Lockout timers • Get alerts when logins fail
Social engineering	• Tricking someone into revealing user data or credentials • "Hi, this is Comcast, can you verify your account information?" • "Hi, this is user X and I forgot my password, can you reset it for me?" • Phishing – making a malicious website look legitimate to entice users to input their data	• Critical thinking – does it make sense that someone would ask you for this info? • Does the website (or URL) look suspicious? • Give info only when you initiate contact • When in doubt, call or email company separately to confirm
Malicious software (malware/virus)	• Tricking user to install by presenting a seemingly-legitimate link • Infected USB drive or network (such as coworker's computer) • Virus can be used for extortion, data extraction, manipulate computer to use for another attack • Examples of commonly exploited programs: Flash, Java, Internet Explorer	• Spam filter • Antivirus software • Gateway antivirus (firewall) on corporate network • Software-based firewall • Do not use your computer as "administrator" unless needed
Internal risk	• Former or current employee has knowledge of username or password • Logs in without detection, since username and password are legitimate • Problem usually not identified until much later – if ever	• Change passwords often • Do not share passwords: "Passwords are like toothbrushes" • Apply access control to data as needed • Audit user account and access control regularly

Prepared by: Dan Lautman, DelCor Technology Solutions