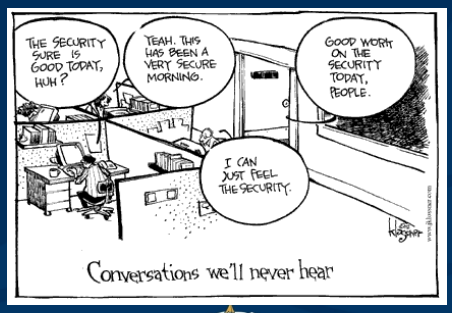
Great Decisions Lecture Series: Cybersecurity in 2012

Dr. Bryson Payne
Chief Information Officer & Associate Professor of Computer Science

Why we're here

- Discussion of personal, business, national and world cybersecurity, and what part you play
- Dr. Payne: Ph.D. in computer science from Georgia State University, sixth year as CIO at North Georgia, past chair of University System of Georgia CIO Advisory Council, USG Audit Advisory Council member, CIO Executive Council, helped organize INTERFACE 2011 Information Security Conference in Atlanta, member of board of directors for North Georgia Network $42M fiber optic broadband co-op

Cybersecurity is hard to grasp...



Topics of Discussion

- Personal Cybersecurity
- Organizational Cybersecurity
- National Cybersecurity
- International/World Cybersecurity
- Things you should know & steps you can take

Personal Cybersecurity Scary Facts

- According to TransUnion:
  - Identity Theft is the fastest growing crime in U.S. (9.9 million incidents a year [FTC])
  - 19 people fall victim to ID theft every **minute**
  - Each crime costs the victim an estimated $500 and 30 hours to resolve, some cases 400+ hours
  - 32% of ID thefts in one study were from family members or relatives, another 18% by friends, neighbors, or in-home employees

Personal Cybersecurity Tips

- Protect your devices – security software & settings (firewall, anti-virus, anti-spyware), passcodes for mobile devices
- Protect your data – beware **spam** & **phishing** emails, know your downloads, shop safely online
- Protect your children – discuss online safety (StaySafeOnline.org), practice safe gaming, monitor social networking, document & report cyber-bullying

Personal Cybersecurity Tips (cont.)

- Become privacy-aware –
  - Who's asking? What are they asking? Why do they need it? "When in doubt, throw it out"
  - Don't over-share, and be aware of your permanent online reputation (post/tweet unto others as…)
  - Use hard passwords, connect with care
- Fix problems quickly – report ID theft, fraud (FTC, FBI Internet Crime Complaint Center), cyber-bullying, harassment, and hacking

NORTH GEORGIA COLLEGE & STATE UNIVERSITY

Good News about Personal Cybersecurity

- Most financial institutions limit loss to $50 or $0, and ID theft coverage can be cheap ($25/yr)
- Most institutions & organizations are helpful in resolving ID theft once reported
- Law enforcement & industry are doing more to identify large-scale ID theft operations
- You can help limit identity theft by being personally aware and documenting/reporting

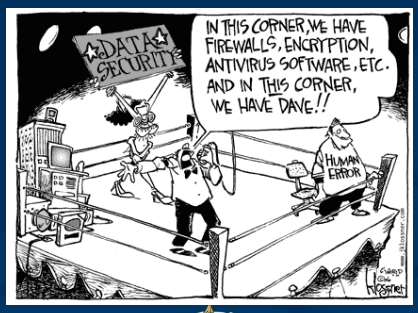
NORTH GEORGIA COLLEGE & STATE UNIVERSITY

Organizational Cybersecurity

- Information Security at work is big business
- Organizations have a duty to protect information that has been entrusted to them
- Includes businesses, non-profits, your kids' soccer team

NORTH GEORGIA COLLEGE & STATE UNIVERSITY

The Front Lines of Business Security…



NORTH GEORGIA COLLEGE & STATE UNIVERSITY

Best Approach: Defense

- Starts with employee awareness (security isn't about technology, it's about people)
- Technology is compromised by inattention, incompetence, and complacency
- Training can pay dividends in dealing with biggest threats: social engineering, mobile and USB device use, weak passwords, carelessness

NORTH GEORGIA COLLEGE & STATE UNIVERSITY

Business Cybersecurity Threats

- Employee negligence (41% of breaches in 2010)
  - Mobile insecurity – up to 12,000 laptops & tablets are lost in US airports **each week** [NSI]
- Malicious or criminal attacks are on the increase (31% in 2010, 24% 2009, 12% 2008)
- System failures accounted for 27% [Ponemon]
- Web site is a main vector of attack – extra security, review of web services are vital

NORTH GEORGIA COLLEGE & STATE UNIVERSITY

Responding to Breaches

- 46 states + DC, PR, and VI have laws requiring notification of security breaches involving PII
- Ponemon Institute reports cost of data breach at $214 per record (how many records are on your laptop/USB drive/unattended computer?)
- Plan ahead for communication & response
- Notify promptly (usually 30 days)

Good news about InfoSec at work

- 2008 research by Carnegie Mellon University found only 1 in 24 large, publicly reported breaches resulted in identity theft
- Most reported breaches are unlikely to lead to identity theft, but can be damaging to business
- Frequent training, risk assessment, encryption & data loss prevention tools & practices greatly reduce the likelihood and cost of data breaches

National Cybersecurity

- Cybersecurity – the new frontier
- Cyberspace and the state
- Explosion of Cybercrime

Cybersecurity: The new frontier

- Cyberspace includes the Internet, as well as all networked information and communications systems worldwide
- Entering a period of intense contestation & potential chaos
- Involves states, civil society, businesses, organized crime and militant groups
- Cybersecurity includes threats both *to* and *through* cyberspace

New frontier (cont.)

- Just over a decade ago, most nations were oblivious to the Internet
- Now, many nations are following the lead of the US in setting up dedicated cyber commands
- Increase in state power coincides with deepening of personal, social & economic impact of connected technologies
  - Facebook: 2004, YouTube: 2005, Twitter: 2006, iPhone: 2007, etc.

Cyberspace and the state

- Who governs the Internet?
  - US Dept of Commerce, delegated corporations, …
  - Recently added Russian & Chinese delegations
  - Role of the private sector
- Critical infrastructure attached to telecommunications networks
- Cloud computing

Explosion of Cybercrime

- Cybercrime is big business – and more organized than ever
- 2011 crime report by Norton suggests cybercrime is $300-400B/year
  - Larger than the global black market for heroin, cocaine and marijuana combined ($288B)
- 80,000 new malware samples are released every day, in addition to targeted attacks

Cybercrime is accelerating

- In June 2011, Thompson Reuters published an "Infographic of the Day" showing 6 months of attacks
- Scope was similar to previous 5-year cyberattack timelines
- One contributing factor is that cybercriminals act globally, but can hide locally

World Cybersecurity

- Changing face of cyberspace
- Cyberspace and the state
- The next battleground
- Good news about US Cybersecurity

Cyberspace is changing

- 44% of the world's Internet users are in Asia (but only 24% of Asians are online…) [FPA]
- 3.8 billion of the 5.3 billion active mobile phone subscriptions are in developing world
- 18 of the top 55 nations in Internet growth rate are considered by UN as "least-developed"
- English has been Internet "operating language", but within 5 years, Chinese could be dominant Internet language

Cyberspace and the state

- Who governs the Internet?
- Filtering and circumvention
- Internet and opposition movements
  - Color revolutions (former USSR), Arab Spring
- International strategies
  - Shanghai Cooperation Organization (SCO) – China, Russia, Kyrgyzstan, Kazakhstan, Tajikistan, Uzbekistan; India, Iran, Pakistan & Mongolia, etc.

The Next Battleground

- Cybercrime sharing techniques with cyber espionage & cyberwarfare
- Distributed denial of service attacks from China – 2005-present; Russian DDoS against Georgia in 2008
- Stuxnet – 2010 computer worm targeted five Iranian organizations associated with uranium enrichment infrastructure

Good news about US Cybersecurity

- In my opinion, we're still #1 in Cybersecurity – but it's a tight race
- Cyberspace is as strategic as land, air, sea, space
- We have some of the smartest individuals, best companies, and strongest government teams on our side
- It's not just a numbers game, but numbers are important – we need more engineers, scientists, technologists

NORTH GEORGIA COLLEGE & STATE UNIVERSITY

Steps you can take...

- For your own identity & information security:
  - Be email-aware, don't fall for phishing or malware
  - Consider Identity Theft insurance ~$25/yr
  - Check your credit report once or twice a year
  - Check your bank/credit card statements often
  - Be privacy-aware, don't over-share
  - Use harder passwords
  - Consider using a standalone machine for financial transactions

NORTH GEORGIA COLLEGE & STATE UNIVERSITY

Steps you can take...

- For your customers' & employees' security:
  - Invest in security awareness training for employees
  - Treat confidential data like "hazardous material" – handle with care, don't just store anywhere
  - Secure your biggest risks first (likely web site, laptops/mobile devices)
  - Prepare for breaches and notifications – have a plan in place for when an event strikes

NORTH GEORGIA COLLEGE & STATE UNIVERSITY

Steps you can take...

- For your country:
  - Encourage young people to go into science, technology, engineering & mathematics (STEM) fields – we need a generation of cyber-heroes!
- The road to security begins with personal responsibility – securing the Internet cannot be outsourced, ignored or forgotten

NORTH GEORGIA COLLEGE & STATE UNIVERSITY

Questions & Discussion

- Added Security Expert:
  - Mr. Jim Webb, Chief Information Security Officer
    North Georgia College & State University
    CISSP, CISM, GSEC

NORTH GEORGIA COLLEGE & STATE UNIVERSITY

Thank you!

- Slides available at www.brysonpayne.com
- Email me at bpayne@northgeorgia.edu
- Follow me at twitter.com/brysonpayne

NORTH GEORGIA COLLEGE & STATE UNIVERSITY