# Security Threats & Trends

Top 10 Major Threats & How to Prevent Them

# The Law & Security

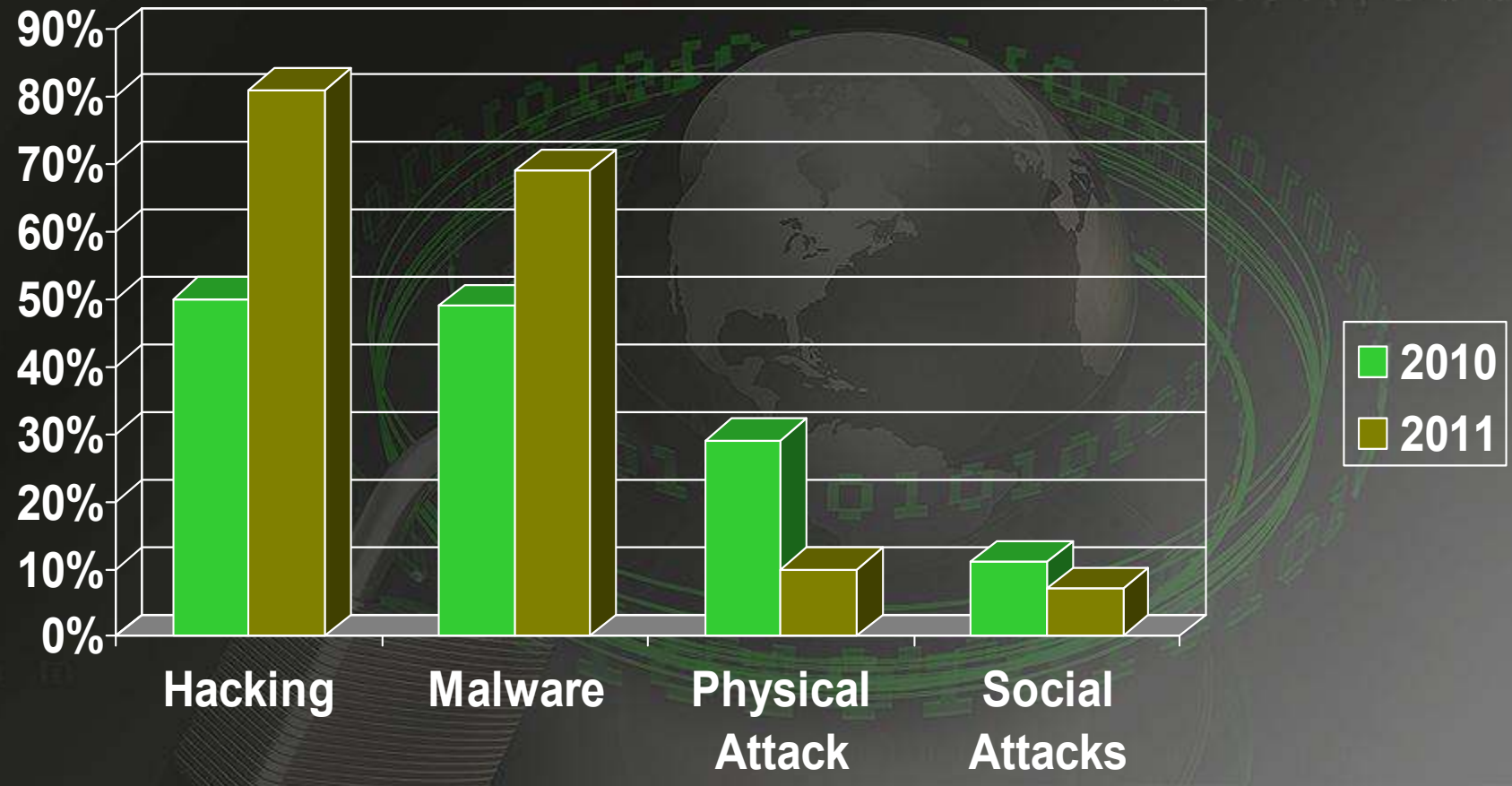
- State Data Breach Notification Laws
- Regulatory / Industry-Specific
  - HIPAA, HITECH
  - GLB, SEC, FACTA
  - FTC
- Commercial Penalties
  - Civil Litigation
  - Negative PR
  - Financial Losses

# 2011 / 2012 Review[1]

- Civil & Cultural Uprising - Hactivism
  - LulzSec
  - Anonymous
  - Cyber Fighters of Izz ad-din Al Qassam
- Sophisticated Cyber Crime
  - Financial Losses Targeted at Specific Industries
- Major Data Breaches
  - 855 Incidents, 174 Million Records (2011)

*1. http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2011_en_xg.pdf*

# How Do Breaches Occur?[1]




*1. http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2011_en_xg.pdf*

# Breach Commonalities[1]

- 96% of attacks were not difficult
- 85% of breaches took weeks to discover
- 92% of incidents discovered by 3rd party
- 97% of incidents were avoidable with simple or intermediate controls

*1. http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2011_en_xg.pdf*

# 10. Social Media / Infected Websites

- Hidden Malware (“Like” button, Apps)
- Malicious code embedded in trusted sites (Watering Hole)
- Social Engineering used to profile the browsing habits of target organizations or people
- *Block Social Media sites internally*
- *Train users of dangers and acceptable usage*
- *Update policies to include social media*
- *Keep systems/software/firmware/ patched*

# 9. Wi-Fi (Secured or Not)

- “Free” hotspots – is it legit?
- Interception of logins or transactions
- Access to file/folder shares
- *Use secure, trusted networks or VPN*
- *Use sound firewalls, AV, HTTPS*
- *Avoid untrusted access points*
- *Make sure all hardware/software is patched, even at deployment*

# 8. AutoRun Exploits (Win XP)

- Autorun.inf compromised
- Default setting in Windows (not Win7 or Win8)
- Runs when portable media is connected
- Excessive permissions = “double-whammy”

- *Disable AutoRun!*
- *Install patch to allow CD’s & DVD’s*

# 7. Over-Confidence in AV

- No such thing as “perfect anti-virus”
- Example = annual flu vaccines
- Also beware of fake anti-virus
- Single layered approach
- *Require frequent auto updates*
- *Don’t rely on just AV; use defense in depth*
- *Train users about fake AV; do not click*

# 6. Lost or Stolen Devices

- Laptops, Smartphones, USB drives
- Data breach notification, privacy laws
- Lost backup tapes
- *Consider encryption technology*
- *Perform vendor due diligence*
- *Include lost/stolen devices in your incident response plan*

# 5. Excessive User Privileges

- Admin rights given to users
- Allows user to intentionally or unintentionally launch applications
- Allows malicious websites or links to launch attacks
- *Do not allow Admin rights for users*
- *Require “least privilege” accounts*

# 4. Poor Password Practices

- Same password used for everything
- Passwords never changed
- Simple, easily guessed passwords
- *Use technology to:*
  - *Force strong passwords*
  - *Force regular password changes*
- *Educate users about passwords*

# 3. Phishing & Spear Phishing

- Disguised links in email
- Social engineering to target specific people
- Uses email, social messaging, or web links
- URL shortening presents new problems
- *Train users on scams continuously*
- *Allow only 1 admin to send out security alerts*
- *Patch systems/AV, control user privileges*

# 2. Unpatched Machines

- Operating System Patches
  - Local machines AND servers AND gear
- 3rd Party App Patches
  - Office, AV, Obscure Apps
- Old exploits still happening
- *Force justification for patch delays*
- *Enable automatic updates (if possible)*

# 1. Data Hostage-Taking

- Hackers encrypt all data of organization
- Send a ransom note & “proof of life”
- Demand ransom be paid for encryption keys
- Medical organizations most recently targeted
- Ransom sent through a series of cyber money mules and offshore hacker banking websites

# 1. Continued

- Loss of data access / billing systems can bankrupt a small business
- *No matter the size of the organization, keep mission critical systems secure*
- *Annual security audits by trusted IT security experts (NOT resellers)*
- *Use SANS Top 20 or HIPAA Security Rule criteria for audit baselines*

# Small Organization Focus[1]

- Implement Firewalls
- Implement Access Control on remote access services
- Change default credentials on all internet facing devices
- Trust but VERIFY – Minimum annual security testing

*1. http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2011_en_xg.pdf*

# Large Organization Focus[1]

- Eliminate unnecessary and / or legacy data
- Monitor logs – outsource / co-source
- Annually review incident response plans – verify with gap analysis
- **Trust but VERIFY – security testing with social engineering, ethical hacking and aggressive penetration testing

1. http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2011_en_xg.pdf

** Not from report – from Reclamere experience

# Questions

Angie Singer Keating, CISA, CIPP, CISM, CRISC
CEO & Co-Founder
814-684-5505 ext. 303
www.reclamere.com
http://www.linkedin.com/in/angiesingerkeating
follow me on Twitter @VeepGeek

RECLAMERE
Data Security Experts